

# Safeguarding Decentralized Wireless Networks Using Full-Duplex Jamming Receivers

Tong-Xing Zheng, *Student Member, IEEE*, Hui-Ming Wang, *Senior Member, IEEE*, Qian Yang, and Moon Ho Lee

**Abstract**—In this paper, we study the benefits of full-duplex (FD) receiver jamming in enhancing the physical-layer security of a two-tier decentralized wireless network with each tier deployed with a large number of pairs of a single-antenna transmitter and a multi-antenna receiver. In the underlying tier, the transmitter sends unclassified information, and the receiver works in the half-duplex (HD) mode receiving the desired signal. In the overlaid tier, the transmitter delivers confidential information in the presence of randomly located eavesdroppers, and the receiver works in the FD mode radiating jamming signals to confuse eavesdroppers and receiving the desired signal simultaneously. We provide a comprehensive performance analysis and network design under a stochastic geometry framework. Specifically, we consider the scenarios where each FD receiver uses single- and multi-antenna jamming, and analyze the connection probability and the secrecy outage probability of a typical FD receiver by providing accurate expressions and more tractable approximations for the two metrics. We further determine the optimal deployment of the FD-mode tier in order to maximize network-wide secrecy throughput subject to constraints including the given dual probabilities and the network-wide throughput of the HD-mode tier. Numerical results are demonstrated to verify our theoretical findings, and show that network-wide secrecy throughput is significantly improved by properly deploying the FD-mode tier.

**Index Terms**—Physical-layer security, decentralized wireless networks (DWNs), full-duplex (FD), multi-antenna, self-interference (SI), outage probability, secrecy throughput, stochastic geometry.

## I. INTRODUCTION

**I**NFORMATION security in wireless communications has attracted prominent attention in the era of information explosion. A traditional approach that safeguards the information security is to use encryption at the upper layers of the communication protocol stack. However, due to the dynamic and large-scale topologies in emerging wireless networks, secret key management and distribution is difficult to implement, especially in a decentralized network architecture without infrastructure [1]. In addition, it might not be practical for low-power network nodes, e.g., sensors, to use complicated cryptographic algorithms [1]. These pose a challenge to securing information delivery solely by means of cryptography-based security mechanisms. Fortunately, *physical-layer security*, a novel approach at the physical layer that achieves secrecy by exploiting the randomness inherent to wireless channels,

has the potential to strengthen network security [2]. Since Wyner's ground-breaking work [3] in which he introduced the *degraded wiretap channel* (DWTC) model and the concept of *secrecy capacity*, physical-layer security has been studied in various wiretap channels models, e.g., multi-input multi-output (MIMO) channels [4], [5], relay channels [6], [7], and two-way channels [8], [9], etc. A comprehensive survey on physical-layer security, including the information-theoretic foundations, the evolution of secure transmission strategies, and potential research directions in this area, can be found in [10].

Early research on physical-layer security is focused on a point-to-point scenario, in which the large-scale fading is ignored when modeling the wireless channels, and as a consequence secure transmissions become irrelevant to the relative spatial locations of legitimate terminals and eavesdroppers. When it comes to a decentralized wireless network (DWN), since each network node suffers great interference from the other nodes spreading over the entire network, network security strongly depends on nodes' spatial positions and propagation path losses. Recently, stochastic geometry theory has provided a powerful tool to analyze network performance by modeling nodes' positions according to a spatial distribution, e.g., a Poisson point process (PPP) [11]–[13]. This has facilitated the research of physical-layer security with randomly distributed legitimate nodes and eavesdroppers in DWNs [14]–[16].

To improve information transfer secrecy, an efficient way is to degrade eavesdroppers' decoding ability by sending jamming signals. Along this line, some efforts have been made. For example, the authors in [14] and [15] consider a single-antenna transmitter scenario, and propose to let the transmitter suspend its own information delivery and act as a friendly jammer to impair eavesdroppers when it is far away from the intended receiver [14] or when eavesdroppers are detected inside its secrecy guard zone [15]. The authors in [16] consider a multi-antenna transmitter scenario, and propose to radiate *artificial noise*<sup>1</sup> with either sectoring or beamforming to confuse eavesdroppers while without impairing the legitimate receiver. Although these endeavors are shown to yield a significant improvement on the secrecy capacity/throughput, they are based on the presence of either multi-antenna transmitters or friendly jammers, which sometimes might not be available. For instance, due to the size and hardware cost constraints, a sensor in a DWN, which transmits sensed data to a data collection

T.-X. Zheng, H.-M. Wang, and Q. Yang are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 710049, Shaanxi, China. Email: txzheng@stu.xjtu.edu.cn, xjbswhm@gmail.com, qian-yang@outlook.com.

M. H. Lee is with the Division of Electronics Engineering, Chonbuk National University, Jeonju 561-756, Korea. Email: moonho@jbnu.ac.kr.

<sup>1</sup> The idea of using artificial noise to interfere with eavesdroppers was first proposed in [17]; this seminal work has unleashed a wave of innovation, mainly including two branches, i.e., multi-antenna techniques [18]–[20] and cooperative jamming strategies [21], [22].

station, is usually equipped with only a single antenna. In addition, a sensor has no extra power to radiate jamming signals due to its low-power constraint. In these scenarios, the jamming schemes proposed in [14]–[16] no longer apply, and it is still challenging to protect information from eavesdropping.

Fortunately, the recent progress of developing in-band full-duplex (FD) radios [26] raises the possibility of enhancing network security in the aforementioned scenarios. In-band FD operation enables a transceiver to simultaneously transmit and receive on the same frequency band. The major challenge in implementing such an FD node is the presence of self-interference (SI) that leaks from the node's output to its input. Nevertheless, thanks to various effective SI cancellation (SIC) techniques, SI can be efficiently mitigated in the analog circuit domain [23], digital circuit domain [24], and spatial domain [25], respectively. FD radios has the potential to improve both link capacity and communication security in DWNs. Returning to the aforementioned scenarios, i.e., with single-antenna sensors and no friendly jammer, using a more powerful FD data collection station provides extra degrees of freedom to protect information delivery, e.g., radiating jamming signals to degrade eavesdroppers while receiving desired signals simultaneously. In particular, when the FD receiver is equipped with multiple antennas, it provides us with potential benefits not only in alleviating SI but also in designing jamming signals.

We point out that sending jamming signals using an FD receiver have already been reported by [27]–[29], where the authors consider single-antenna receiver jamming with SI perfectly canceled in a cost-free manner, consider multi-antenna receiver jamming with SI taken into account, and consider both transmitter and receiver jamming, respectively. However, these works are confined to a point-to-point scenario. When considering a DWN, analyzing the influence of FD radios on network security becomes much more sophisticated due to the presence of not only the mutual interference between nodes but also the SI. To the best of our knowledge, the potential advantages of FD jamming in the context of physical-layer security from a network perspective are elusive, and a fundamental mathematical framework for performance analysis and network design is lacking, which has motivated our work.

#### A. Our Work and Contributions

In this paper, we investigate the physical-layer security of a two-tier heterogeneous DWN under a stochastic geometry framework, where single-antenna transmitters (sensors) and multi-antenna receivers (data collection stations) in each tier are organized in pairs. The first tier is an underlying tier that has no secrecy requirement and each receiver therein works in the half-duplex (HD) mode. The second tier is an overlaid tier that has secrecy considerations and is deployed with more powerful FD receivers. For convenience, we name the two tiers the HD tier and the FD tier throughout the paper, respectively. Randomly located multi-antenna eavesdroppers intend to wiretap the secrecy data flowing in the FD tier. The reasons why we consider this model are:

- This model characterizes a practical communication scenario where a security-oriented network is newly de-

ployed over an existing network that has no security requirement. For example, a military ad hoc network specifically for secret information exchange such as offensive tactics, is momentarily added to a civilian ad hoc network, or an unlicensed security secondary tier in an underlay cognitive radio network should make its interference to the primary tier under control to guarantee smooth communications for the latter.

- This is a more general DWN model that incorporates communications with and without security requirements. The secure decentralized ad hoc network models discussed in [15] and [16] are just special cases of our model when we simply put aside the HD tier.
- In addition, investigating the achievable performances in such a two-tier heterogeneous network facilitates us to gain a better understanding of the interplay between the classified and unclassified networks, and to evaluate the impact of FD jamming to an existing communication network without security constraint.

The main contributions of this paper are summarized as follows:

- We analyze the connection probability and the secrecy outage probability of a typical FD receiver under a spatial SIC (SSIC) strategy, and provide accurate integral expressions as well as analytical approximations for the given metrics. We show that deploying more FD nodes introduces greater interference to the network, which not only decreases the connection probability but also decreases the secrecy outage probability.
- We study the optimal deployment of the FD tier to maximize network-wide secrecy throughput subject to constraints including the connection probability, the secrecy outage probability, and the HD tier throughput. In particular, when the FD receiver uses single-antenna jamming, we prove the *quasi-concavity* of the secrecy throughput with respect to (w.r.t.) the FD tier density; the optimal density that maximizes secrecy throughput can be obtained using the bisection method.
- For the multi-antenna jamming scenario, we investigate how the number of jamming signal streams and the number of jamming antennas affect secrecy throughput. We reveal that increasing jamming signal streams always benefits secrecy throughput. However, whether adding jamming antennas is advantageous or not depends on specific communication environments. A proper number of jamming antennas should be chosen to balance transmission reliability with secrecy.

#### B. Organization and Notations

The remainder of this paper is organized as follows. In Section II, we describe the system model and the underlying optimization problem. In Sections III and IV, we provide performance analysis and network design in single-antenna jamming and multi-antenna jamming scenarios, respectively. In Section V, we conclude our work.

*Notations:* bold uppercase (lowercase) letters denote matrices (vectors).  $(\cdot)^H$ ,  $|\cdot|$ ,  $\|\cdot\|$ ,  $\mathbb{P}\{\cdot\}$ , and  $\mathbb{E}_A(\cdot)$  denote Hermitian transpose, absolute value, Euclidean norm, probability,

TABLE I: Key Symbols Used in the Paper

Symbols	Definition/Explanation
$\Phi_h, \Phi_f$	PPPs for RxS in HD and FD tiers
$\hat{\Phi}_h, \hat{\Phi}_f$	PPPs for TxS in HD and FD tiers
$\Phi_e$	PPP for eavesdroppers
$\lambda_h, \lambda_f, \lambda_e$	Densities of PPPs $\Phi_h$ ( $\hat{\Phi}_h$ ), $\Phi_f$ ( $\hat{\Phi}_f$ ) and $\Phi_e$
$N_h, N_f$	Numbers of antennas at HD and FD RxS
$N_e$	Number of antennas at an eavesdropper
$N_t$	Number of jamming antennas at an FD Rx
$N_j$	Number of jamming signal streams at an FD Rx
$P_h, P_f$	Transmit powers at TxS in the HD and FD tiers
$P_t$	Power of jamming signals at an FD Rx
$(x, \hat{x})$	Locations of a Rx and its paired Tx
$D_h, D_f$	Distances between Tx-Rx pairs in HD and FD tiers
$D_{xy}$	Distance between a node at $x$ and a node at $y$
$\mathcal{P}_c, \mathcal{P}_t$	Connection probabilities of HD and FD RxS
$\mathcal{P}_{so}$	Secrecy outage probability of an FD Rx
$\mathcal{T}_s$	Network-wide secrecy throughput of the FD tier
$\mathcal{T}_c$	Network-wide throughput of the HD tier

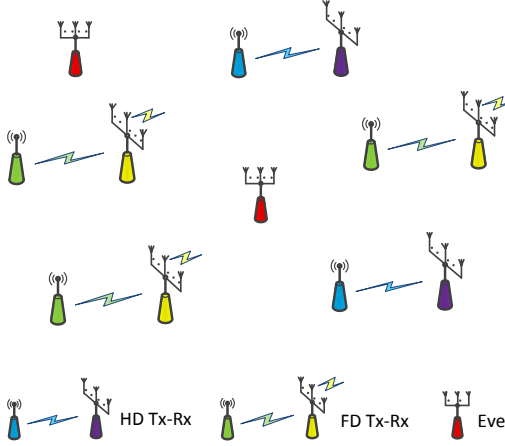


Fig. 1: An illustration of a two-tier heterogeneous DWN consisting of both HD and FD tiers. Each HD (FD) Rx receives data from an intended Tx. The ongoing transmission between the FD Tx-Rx pair is overheard by randomly located eavesdroppers (Eves).

and expectation w.r.t.  $A$ , respectively.  $\mathcal{CN}(\mu, \nu)$ ,  $\text{Exp}(\lambda)$  and  $\Gamma(N, \lambda)$  denote the circularly symmetric complex Gaussian distribution with mean  $\mu$  and variance  $\nu$ , exponential distribution with parameter  $\lambda$ , and gamma distribution with parameters  $N$  and  $\lambda$ , respectively.  $\mathbb{C}^{m \times n}$  denotes the  $m \times n$  complex number domain.  $\log(\cdot)$  and  $\ln(\cdot)$  denote the base-2 and natural logarithms, respectively.  $f^{(m)}$  denotes the  $m$ -order derivative of  $f$ .  $[x]^+ \triangleq \max(x, 0)$ . The key symbols used in the paper are listed in Table I.

## II. SYSTEM MODEL

Consider a two-tier heterogeneous DWN in which an existing tier that provides unclassified services is overlaid with a temporarily deployed tier that has classified services. In either tier, each data source (Tx) has only a single antenna due to hardware cost, and reports data up to its paired data collection station (Rx); each Rx is equipped with multiple antennas for signal enhancement, interference suppression, information protection, etc. In the underlying tier, the Tx sends an unclassified message to the Rx, and the latter works in the HD mode, using

all its antennas to receive the desired signal. In the overlaid tier, the Tx delivers a confidential message to its Rx in the presence of randomly located eavesdroppers, and the Rx works in the FD mode, simultaneously using part of its antennas to receive the desired signal and using the remaining to radiate jamming signals to confuse eavesdroppers. An illustration of a network snapshot is depicted in Fig. 1. We model the locations of HD RxS, FD RxS and eavesdroppers according to independent homogeneous PPPs  $\Phi_h$  with density  $\lambda_h$ ,  $\Phi_f$  with density  $\lambda_f$ , and  $\Phi_e$  with density  $\lambda_e$ , respectively. We further use  $\hat{\Phi}_h$  and  $\hat{\Phi}_f$  to denote the sets of locations of the TxS in the HD and FD tiers, which also obey independent PPPs with densities  $\lambda_h$  and  $\lambda_f$  according to the displacement theorem [35, page 35]. Wireless channels are assumed to experience a large-scale path loss governed by the exponent  $\alpha > 2$  along with flat Rayleigh fading with fading coefficients independent and identically distributed (i.i.d.) obeying  $\mathcal{CN}(0, 1)$ . We assume that each Rx knows the channel state information of its paired Tx. Since each eavesdropper passively receives signals, its channel state information is unknown, whereas its channel statistics information is available, see e.g., [12]–[28].

Without loss of generality, we consider a typical Tx-Rx pair in the FD tier and place the Rx at the origin  $o$  of the coordinate system<sup>2</sup>. Note that the aggregate interferences received at the typical FD Rx consist of the undesired signals from all the TxS (except for the typical Tx) and the jamming signals from itself and from all the other FD RxS. The received signal of the typical FD Rx is given by

$$\begin{aligned}
 y_f = & \underbrace{\frac{\sqrt{P_f} \mathbf{f}_{\hat{o}o} s_{f,\hat{o}}}{D_f^{\alpha/2}}}_{\text{desired signal}} + \underbrace{\sqrt{P_t} \mathbf{F}_{oo} \mathbf{v}_o}_{\text{SI}} + \underbrace{\sum_{\hat{z} \in \hat{\Phi}_h} \frac{\sqrt{P_h} \mathbf{f}_{\hat{z}o} s_{h,\hat{z}}}{D_{\hat{z}o}^{\alpha/2}}}_{\text{HD-tier undesired signals}} \\
 & + \underbrace{\sum_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} \left( \frac{\sqrt{P_f} \mathbf{f}_{\hat{z}o} s_{f,\hat{z}}}{D_{\hat{z}o}^{\alpha/2}} + \frac{\sqrt{P_t} \mathbf{F}_{zo} \mathbf{v}_z}{D_{zo}^{\alpha/2}} \right)}_{\text{FD-tier undesired and jamming signals}} + \mathbf{n}_f, \quad (1)
 \end{aligned}$$

where  $s_{f,\hat{z}}$  ( $s_{h,\hat{z}}$ ) denotes the signal from the Tx located at  $\hat{z}$  in the FD (HD) tier with  $\mathbb{E}[|s_{f,\hat{z}}|^2] = 1$  ( $\mathbb{E}[|s_{h,\hat{z}}|^2] = 1$ );  $\mathbf{v}_z \in \mathbb{C}^{N_t \times 1}$  denotes a jamming signal vector from the FD Rx at  $z$  with  $\mathbb{E}[\|\mathbf{v}_z\|^2] = 1$ ;  $\mathbf{n}$  denotes thermal noise;  $P_f$ ,  $P_h$  and  $P_t$  denote the transmit powers of the TxS in the FD tier, in the HD tier, and of the FD RxS, respectively;  $\mathbf{f}_{xy} \in \mathbb{C}^{(N_f - N_t) \times 1}$  ( $\mathbf{F}_{xy} \in \mathbb{C}^{(N_f - N_t) \times N_t}$ ) denotes the small-scale fading coefficient vector (matrix) of the channel from the node at  $x$  to the FD Rx at  $y$  ( $\mathbf{F}_{oo}$  denotes the SI channel matrix related to the residual SI after passive SI suppression like antenna isolation, the entries of which can be regarded as independent Rayleigh distributed variables [30]). It is worth noting that, due to the fixed Tx-Rx pair separation distance  $D_f$ <sup>3</sup>,  $D_{\hat{z}o}$  and  $D_{zo}$  in (1) are not independent;  $D_{\hat{z}o}$  can be

<sup>2</sup>From Slivnyak's theorem [36], the spatial distribution of all the other nodes will not be affected.

<sup>3</sup>Fixing the Tx-Rx pair distance is quite generic when dealing with a DWN with or without security considerations [15], [16], [31], [32], which allows us to ease the mathematical analysis. Nevertheless, the results obtained under this hypothesis can be easily extended to an arbitrary distribution of  $D_f$ , as referred to [11].

expressed by  $D_{\hat{z}o} = \sqrt{D_{zo}^2 + D_f^2 - 2D_{zo}D_f \cos \theta_z}$ , where the angle  $\theta_z$  is uniformly distributed in the range  $[0, 2\pi]$ . As can be seen in subsequent analysis, the correlation between  $D_{\hat{z}o}$  and  $D_{zo}$  makes it challenging to derive analytically tractable results for involved performance metrics.

As to the HD Rx located at  $b$ , since it suffers no SI, the received signal is given by

$$\mathbf{y}_h = \frac{\sqrt{P_h} \mathbf{h}_{\hat{o}o} s_{h,\hat{o}}}{D_h^{\alpha/2}} + \sum_{\hat{z} \in \hat{\Phi}_h \setminus \hat{o}} \frac{\sqrt{P_h} \mathbf{h}_{\hat{z}o} s_{h,\hat{z}}}{D_{\hat{z}o}^{\alpha/2}} + \sum_{\hat{z} \in \hat{\Phi}_f} \left( \frac{\sqrt{P_f} \mathbf{h}_{\hat{z}o} s_{f,\hat{z}}}{D_{\hat{z}o}^{\alpha/2}} + \frac{\sqrt{P_t} \mathbf{H}_{zo} \mathbf{v}_z}{D_{zo}^{\alpha/2}} \right) + \mathbf{n}_h, \quad (2)$$

where  $\mathbf{h}_{xy} \in \mathbb{C}^{N_h \times 1}$  ( $\mathbf{H}_{xy} \in \mathbb{C}^{N_h \times N_t}$ ) denotes the small-scale fading coefficient vector (matrix) of the channel from the node at  $x$  to the HD Rx at  $y$ .

Similarly, for the eavesdropper located at  $e$  that is intended to wiretap the data transmission from the typical Tx to the typical FD Rx, the received signal is given by

$$\mathbf{y}_e = \frac{\sqrt{P_f} \mathbf{g}_{\hat{o}e} s_{f,\hat{o}}}{D_{\hat{o}e}^{\alpha/2}} + \frac{\sqrt{P_t} \mathbf{G}_{oe} \mathbf{v}_o}{D_{oe}^{\alpha/2}} + \sum_{\hat{z} \in \hat{\Phi}_h} \frac{\sqrt{P_h} \mathbf{g}_{\hat{z}e} s_{h,\hat{z}}}{D_{\hat{z}e}^{\alpha/2}} + \sum_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} \left( \frac{\sqrt{P_f} \mathbf{g}_{\hat{z}e} s_{f,\hat{z}}}{D_{\hat{z}e}^{\alpha/2}} + \frac{\sqrt{P_t} \mathbf{G}_{ze} \mathbf{v}_z}{D_{ze}^{\alpha/2}} \right) + \mathbf{n}_e, \quad (3)$$

with  $\mathbf{g}_{xe} \in \mathbb{C}^{N_e \times 1}$  ( $\mathbf{G}_{xe} \in \mathbb{C}^{N_e \times N_t}$ ) the fading coefficient vector (matrix) of the link from the node at  $x$  to the eavesdropper at  $e$  and  $\sqrt{P_t} \mathbf{G}_{oe} \mathbf{v}_o D_{oe}^{-\alpha/2}$  the interference from the typical FD Rx.

#### A. Wiretap Encoding and Performance Metrics

We consider a non-colluding wiretap scenario in which eavesdroppers do not cooperate with each other and each eavesdropper individually decodes a secret message. To safeguard information security, we utilize the well-known Wyner's wiretap encoding scheme [3] to encode secret information. Let  $R_t$  and  $R_s$  denote the rates of the transmitted codewords and the embedded secret messages, and  $R_e \triangleq R_t - R_s$  denote the rate of redundant information that is exploited to provide secrecy against eavesdropping. If a Tx-Rx link can support the rate  $R_t$ , the Rx is able to decode the secret messages; this corresponds to a reliable connection event [15]. The connection probability of a typical FD Rx is defined as the probability that the signal-to-interference-plus-noise ratio (SINR) of the FD Rx, denoted by  $\text{SINR}_f$ , lies above an SINR threshold  $\beta_t \triangleq 2^{R_t} - 1$ , i.e.,

$$\mathcal{P}_t \triangleq \mathbb{P}\{\text{SINR}_f > \beta_t\}. \quad (4)$$

Similarly, the connection probability of an HD Rx is defined by  $\mathcal{P}_c \triangleq \mathbb{P}\{\text{SINR}_h > \beta_c\}$ , where  $\beta_c \triangleq 2^{R_c} - 1$  with  $R_c$  the corresponding codeword rate.

If the channel from the Tx to any of the eavesdroppers can support the redundant rate  $R_e$ , perfect secrecy is compromised and a secrecy outage event occurs [16]. The secrecy outage probability is defined as the complement of the probability

that the SINR of an arbitrary eavesdropper at  $e$ , denoted by  $\text{SINR}_e$ , lies below an SINR threshold  $\beta_e \triangleq 2^{R_e} - 1$ , i.e.,

$$\mathcal{P}_{so} \triangleq 1 - \mathbb{E}_{\Phi_e} \left[ \prod_{e \in \Phi_e} \mathbb{P}\{\text{SINR}_e < \beta_e | \Phi_e\} \right]. \quad (5)$$

To evaluate the efficiency of secure transmissions in a DWN, we focus on the performance metric named *network-wide secrecy throughput* (unit: bits/s/Hz/m<sup>2</sup>), which is defined as the averagely successfully transmitted information bits per second per Hertz per unit area under a connection probability  $\mathcal{P}_t(\beta_t) = \sigma$  and a secrecy outage probability  $\mathcal{P}_{so}(\beta_e) = \epsilon$  [15], [16], i.e.,

$$\begin{aligned} \mathcal{T}_s &\triangleq \lambda_f \sigma \mathcal{R}_s^* = \lambda_f \sigma [\mathcal{R}_t^* - \mathcal{R}_e^*]^+ \\ &= \lambda_f \sigma [\log(1 + \beta_t^*) - \log(1 + \beta_e^*)]^+. \end{aligned} \quad (6)$$

In (6),  $R_t^* \triangleq \log(1 + \beta_t^*)$ ,  $R_e^* \triangleq \log(1 + \beta_e^*)$  and  $R_s^* = R_t^* - R_e^*$  denote the codeword rate, redundant rate and secrecy rate at a Tx in the FD tier, with  $\beta_t^*$  and  $\beta_e^*$  satisfying  $\mathcal{P}_t(\beta_t) = \sigma$  and  $\mathcal{P}_{so}(\beta_e) = \epsilon$ , respectively. Likewise, the network-wide throughput of the HD tier under a connection probability  $\mathcal{P}_c(\beta_c) = \sigma_c$  is defined by  $\mathcal{T}_c \triangleq \lambda_h \sigma_c R_c^*$ , where  $R_c^* \triangleq \log(1 + \beta_c^*)$  with  $\beta_c^*$  satisfying  $\mathcal{P}_c(\beta_c) = \sigma_c$ .

We emphasize that the FD tier density strikes a non-trivial tradeoff between spatial reuse, reliable connection, and safeguarding. On one hand, increasing the density of the FD tier establishes more communication links per unit area, potentially increasing throughput; meanwhile, the increased jamming signals introduced by newly deployed FD Rxs greatly degrade the wiretap channels. On the other hand, the additional amount of interference caused by adding new devices deteriorates ongoing receptions, decreasing the probability of successfully connecting Tx-Rx pairs. The overall balance of such opposite effects on secrecy throughput needs to be carefully addressed. Note that, from a network perspective, network designers may concern themselves more with the network deployment rather than optimizing other parameters like transmit or jamming power, antenna number, etc. For example, in a security monitoring wireless sensor network, network designers may fix the transmit power of sensor nodes to their maximum values for simplicity, but would modestly design how many sensors should be scattered in order to satisfy the monitoring requirement. Therefore, in this paper, we aim to determine the deployment of the FD tier to achieve the maximum network-wide secrecy throughput while guaranteeing a certain level of network-wide throughput for the HD tier.

In the following sections, we deal with network design by considering the scenarios of each FD Rx using single-antenna (SA) jamming ( $N_t = 1$ ) and using multi-antenna (MA) jamming ( $N_t > 1$ ), respectively. The reason behind such a division is threefold:

1) In the SA case, SSIC can only be operated at the FD Rx's input using a hybrid zero-forcing and maximal ratio combining (ZF-MRC) criterion; in the MA case, due to the extra degrees of freedom, the FD Rx simply performs SSIC at the output and just adopts the MRC reception at the input.

2) In the SA case, since the channel from the FD receiver's output to either the legitimate node or to the eavesdropper

is a single-input multi-output channel, it is relatively easy to analyze connection probability and secrecy outage probability; in the MA case, either of the above channels is an MIMO channel, which makes the analysis much more complicated, e.g., analyzing the secrecy outage probability requires using the theory from integer partitions.

3) In the SA case, we prove the quasi-concavity of network-wide secrecy throughput w.r.t. the FD tier density, and calculate the optimal FD tier density that maximizes network-wide secrecy throughput using the bisection method; in the MA case, due to the analytically intractable integer partitions, we can only obtain the peak network-wide secrecy throughput via one-dimensional exhaustive search.

In our analysis, due to uncoordinated concurrent transmissions, the aggregate interference at a receiver dominates thermal noise. For tractability, we consider the *interference-limited* case by ignoring thermal noise. Nevertheless, our results can be easily generalized to the case with thermal noise. For ease of notation, we define  $\delta \triangleq 2/\alpha$ ,  $C_{\alpha,N} \triangleq \frac{\pi\Gamma(N-1+\delta)\Gamma(1-\delta)}{\Gamma(N-1)}$ , and  $P_{ab} \triangleq P_a/P_b$  for  $a, b \in \{h, f, t\}$ .

### III. SINGLE-ANTENNA-JAMMING FD RECEIVER

In this section, we consider the scenario where each FD Rx uses single-antenna jamming, i.e.,  $N_t = 1$ . Thereby, matrices  $\mathbf{F}$ ,  $\mathbf{H}$  and  $\mathbf{G}$  given in (1)-(3) reduce to vectors  $\mathbf{f}$ ,  $\mathbf{h}$ , and  $\mathbf{g}$ , respectively, and vector  $\mathbf{v}$  reduces to scalar  $v$ . Without loss of generality, we consider a typical FD Tx-Rx pair  $(\hat{o}, o)$ . We first analyze the connection probability and the secrecy outage probability of the typical FD Rx, and then maximize network-wide secrecy throughput by optimizing the density of the FD tier.

To counteract the SI and simultaneously strengthen the desired signal, the weight vector  $\mathbf{w}_f$  at the FD Rx's input can be chosen according to a hybrid ZF-MRC criterion<sup>4</sup>, which is

$$\mathbf{w}_f = \frac{\mathbf{f}_{\hat{o}o}^H \mathbf{U} \mathbf{U}^H}{\|\mathbf{f}_{\hat{o}o}^H \mathbf{U}\|}, \quad (7)$$

where  $\mathbf{U} \in \mathbb{C}^{(N_f-1) \times (N_f-2)}$  is the projection matrix onto the null space of vector  $\mathbf{f}_{\hat{o}o}^H$  such that the columns of  $\left[\frac{\mathbf{f}_{\hat{o}o}^H}{\|\mathbf{f}_{\hat{o}o}^H\|}, \mathbf{U}\right]$  constitute an orthogonal basis. In this way, we have  $\mathbf{w}_f^H \mathbf{f}_{\hat{o}o} = 0$ .

#### A. Connection Probability

In this subsection, we investigate the connection probability of the typical FD Rx. From (1) and (7), the SIR of the typical FD Rx is given by

$$\text{SIR}_f = \frac{P_f \|\mathbf{f}_{\hat{o}o}^H \mathbf{U}\|^2 D_f^{-\alpha}}{I_h + I_f}, \quad (8)$$

where  $I_h \triangleq \sum_{\hat{z} \in \hat{\Phi}_h} P_h |\mathbf{w}_f^H \mathbf{f}_{\hat{z}o}|^2 D_{\hat{z}o}^{-\alpha}$  and  $I_f \triangleq \sum_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} (P_f |\mathbf{w}_f^H \mathbf{f}_{\hat{z}o}|^2 D_{\hat{z}o}^{-\alpha} + P_t |\mathbf{w}_f^H \mathbf{f}_{\hat{z}o}|^2 D_{\hat{z}o}^{-\alpha})$  are the

<sup>4</sup>ZF-MRC receiver might not be the optimal one, but it is really a simple yet efficient alternative that yields an achievable secrecy rate/throughput. Limiting the receiver in the null space of SI successfully avoids the SI invasion in the spatial domain without consuming extra circuit power that would be used for SI cancellation in the analog or digital domain.

aggregate interferences from the HD tier and FD tier, respectively. In the following theorem, we provide a general expression of the exact connection probability  $\mathcal{P}_t$ .

*Theorem 1:* The connection probability of a typical FD Rx is

$$\mathcal{P}_t = \sum_{m=0}^{N_f-3} \frac{(-1)^m}{m!} \left( \frac{D_f^\alpha \beta_t}{P_f} \right)^m \times \left( e^{-\lambda_h C_{\alpha,2}(P_h s)^\delta} \mathcal{L}_{I_f} \left( D_f^\alpha \beta_t / P_f \right) \right)^{(m)}, \quad (9)$$

where  $\mathcal{L}_{I_f}(s)$  denotes the Laplace transform of  $I_f$ , i.e.,

$$\mathcal{L}_{I_f}(s) = \exp \left( -\lambda_f \int_0^\infty \left( 2\pi - \int_0^{2\pi} \frac{1}{1 + P_f s r^{-\alpha}} \times \frac{d\theta}{1 + P_t s (r^2 + D_f^2 - 2r D_f \cos \theta)^{-\alpha/2}} \right) r dr \right). \quad (10)$$

*Proof:* Please see Appendix A. ■

Theorem 1 provides an exact connection probability without requiring time-consuming Monte Carlo simulations. A special case is that when  $N_f = 3$ ,  $\mathcal{P}_t$  simplifies to  $e^{-\lambda_h C_{\alpha,2}(P_h s)^\delta} \mathcal{L}_{I_f} \left( D_f^\alpha \beta_t / P_f \right)$ . However, for the more general case, the double integral term in (10) makes computing  $\mathcal{L}_{I_f}^{(m)}(s)$  quite difficult, thus making (9) rather unwieldy to analyze. This motivates the need for more compact forms, and in the following theorem we provide closed-form lower and upper bounds for  $\mathcal{P}_t$ .

*Theorem 2:* The connection probability  $\mathcal{P}_t$  of a typical FD Rx is lower bounded by  $\mathcal{P}_t^L$  and upper bounded by  $\mathcal{P}_t^U$ ; which share the same closed form given below,

$$\mathcal{P}_t^S = e^{-\Lambda_f^S \beta_t^\delta} + e^{-\Lambda_f^S \beta_t^\delta} \sum_{m=1}^{N_f-3} \frac{1}{m!} \times \sum_{n=1}^m (\delta \Lambda_f^S \beta_t^\delta)^n \Upsilon_{m,n}, \quad \forall S \in \{L, U\} \quad (11)$$

where  $\Lambda_f^L \triangleq C_{\alpha,2} D_f^2 \left( P_{hf}^\delta \lambda_h + (1 + P_{tf}^\delta) \lambda_f \right)$ ,  $\Lambda_f^U \triangleq C_{\alpha,2} D_f^2 \left( P_{hf}^\delta \lambda_h + \frac{1+\delta}{2} (1 + P_{tf}^\delta) \lambda_f \right)$  and  $\Upsilon_{m,n} = \sum_{\psi_j \in \text{comb}_{m-n}^{(m-1)}} \prod_{i=1, \dots, m-n}^{l_{ij} \in \psi_j} (l_{ij} - \delta(l_{ij} - i + 1))$ . Here  $\text{comb}_{m-n}^{(m-1)}$  denotes the set of all distinct subsets of the natural numbers  $\{1, 2, \dots, m-1\}$  with cardinality  $m-n$ . The elements in each subset are arranged in an increasing order with  $l_{ij}$  the  $i$ -th element of  $\psi_j$ . For  $m \geq 1$ , we have  $\Upsilon_{m,m} = 1$ .

*Proof:* Please see Appendix B. ■

Although (11) still seems complicated, it is actually very easy to compute without any integrals. Considering a practical need of a high level of reliability, we concentrate on the large probability region in which  $\mathcal{P}_t^S \rightarrow 1$  for  $S \in \{L, U\}$ , and provide a much simpler approximation for  $\mathcal{P}_t^S$  in the following corollary, which further facilitates the analysis.

*Corollary 1:* In the large probability region, i.e.,  $\mathcal{P}_t \rightarrow 1$ ,  $\mathcal{P}_t^S$  in (11) is approximated by

$$\mathcal{P}_t^S \approx 1 - \Lambda_f^S \beta_t^\delta K_{\alpha, N_f-2}, \quad \forall S \in \{L, U\} \quad (12)$$

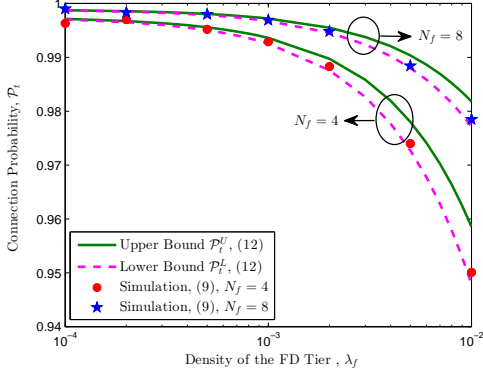


Fig. 2: Connection probability vs.  $\lambda_f$  for different values of  $N_f$ , with  $P_t = 0\text{dBm}$ ,  $N_t = 1$ , and  $\beta_t = 1$ . Unless specified otherwise, we set  $\alpha = 3.5$ ,  $P_f = P_h = 0\text{dBm}$ ,  $N_h = 4$ ,  $\lambda_h = 10^{-3}$  and  $D_f = D_h = 1$ .

where  $K_{\alpha,N} = 1 + \sum_{m=1}^{N-1} \frac{1}{m!} \prod_{l=0}^{m-1} (l - \delta)$ .

*Proof:* We see from (11) that  $\mathcal{P}_t^S \rightarrow 1$  as  $\Lambda_f^S \rightarrow 0$ . Here,  $\Lambda_f^S \rightarrow 0$  reflects all cases of system parameters such as  $D_f$ ,  $\lambda_f$  and  $\lambda_h$  that may lead to a large  $\mathcal{P}_t^S$ . A reasonable case of  $\Lambda_f^S \rightarrow 0$  is but is not limited to that the Tx-Rx pair distance is much less than the average distance between any two Tx (or between two Rx), i.e.,  $D_f^2 \lambda_f, D_f^2 \lambda_h \ll 1$ . Using the first-order Taylor expansion with (11) around  $\Lambda_f^S = 0$  and discarding the high order terms  $\Theta\left(\left(\Lambda_f^S\right)^2\right)$ , we complete the proof. ■

The bound results given in Corollary 1 are shown in Fig. 2, in which we see in the large probability region the lower bound  $\mathcal{P}_t^L$  is tight to the exact value of  $\mathcal{P}_t$  from Monte-Carlo simulations. Therefore in subsequent analysis, we focus on the lower bound  $\mathcal{P}_t^L$  instead of  $\mathcal{P}_t$ . Note that this is actually a pessimistic evaluation of real connection performance. From Fig. 2, we also find that connection performance deteriorates as the FD tier density  $\lambda_f$  increases due to the additional amount of interference. This is ameliorated by adding receive antennas at the FD Rx.

Comparing (2) with (1), it is not difficult to conclude that the connection probability  $\mathcal{P}_c$  of a typical HD Rx shares a similar form as  $\mathcal{P}_t$ . Likewise, we can obtain an approximation for  $\mathcal{P}_c$  in the large probability region, which is provided by the following corollary.

*Corollary 2:* Define  $\Lambda_h \triangleq C_{\alpha,2} \left( \lambda_h + \left( P_{fh}^\delta + P_{th}^\delta \right) \lambda_f \right) D_h^2$ . In the large probability region, the connection probability  $\mathcal{P}_c$  of a typical HD Rx is approximated by

$$\mathcal{P}_c \approx 1 - \Lambda_h \beta_c^\delta K_{\alpha,N_h}. \quad (13)$$

## B. Secrecy Outage Probability

In this subsection, we investigate the secrecy outage probability which corresponds to the probability that a secret message is decoded by *at least* one eavesdropper in the network.

To guarantee secrecy, we should not underestimate the wiretap capability of eavesdroppers. Thereby, we consider a worst-case wiretap scenario assuming that all eavesdroppers have

multiuser decoding capabilities (e.g., successive interference cancellation), thus each eavesdropper itself can successfully resolve the signals radiated from those unexpected transmitters and remove them from its received signals<sup>5</sup> [16]. In this way, the aggregate interference received at each eavesdropper only consists of the jamming signals emitted by all the FD Rxs. We assume that eavesdroppers use the optimal linear receiver, i.e., the minimum mean square error (MMSE) receiver [33], to strengthen the received signals. From (3), the weight vector of the eavesdropper located at  $e$  when using the MMSE receiver is

$$\mathbf{w}_e = \mathbf{R}_e^{-1} \mathbf{g}_{oe}, \quad (14)$$

where  $\mathbf{R}_e \triangleq P_t \mathbf{g}_{oe} \mathbf{g}_{oe}^H D_{oe}^{-\alpha} + \sum_{z \in \Phi_f \setminus o} P_t \mathbf{g}_{ze} \mathbf{g}_{ze}^H D_{ze}^{-\alpha}$ , and the resulting SIR is given by

$$\text{SIR}_e = P_f \mathbf{g}_{oe}^H \mathbf{R}_e^{-1} \mathbf{g}_{oe} D_{oe}^{-\alpha}. \quad (15)$$

In the following theorem, we provide a general expression of the exact secrecy outage probability.

*Theorem 3:* The secrecy outage probability  $\mathcal{P}_{so}$  of a typical FD Rx is

$$\mathcal{P}_{so} = 1 - \exp \left( - \lambda_e \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,1)} \frac{\left( C_{\alpha,2} \lambda_f (P_{tf} \beta_e)^\delta \right)^{n-i}}{(n-i)!} \int_0^\infty \mathcal{Q}_i(r) r^{2(n-i)} e^{-C_{\alpha,2} \lambda_f (P_{tf} \beta_e)^\delta r^2} r dr \right), \quad (16)$$

where  $\mathcal{Q}_i(r) = \int_0^{2\pi} \frac{(P_{tf} \beta_e (r / \sqrt{r^2 + D_f^2 - 2r D_f \cos \theta})^\alpha)^i}{1 + P_{tf} \beta_e (r / \sqrt{r^2 + D_f^2 - 2r D_f \cos \theta})^\alpha} d\theta$ .

*Proof:* Please see Appendix C. ■

The double integral in (16) makes  $\mathcal{P}_{so}$  difficult to analyze. Note that, in a large-scale DWN, a Tx is generally a simple node with low transmit power, e.g., a sensor, and has very short coverage. Therefore, to guarantee a reliable communication and meanwhile protect information from eavesdropping, the separation distance  $D_f$  between a Tx-Rx pair is usually set small. In view of this, in order to develop useful and meanwhile tractable insights into the behavior of the secrecy outage probability  $\mathcal{P}_{so}$ , we resort to an asymptotic analysis by considering a small  $D_f$  regime, e.g.,  $D_f \rightarrow 0$ , and provide quite a simple approximation for  $\mathcal{P}_{so}$  in Corollary 3. We stress that, although Corollary 3 is obtained by assuming  $D_f \rightarrow 0$ , it applies more generally. As can be seen in Fig. 3, (17) provides a very accurate approximation for the exact value in (16) for quite a wide range of  $D_f$ . This illustrates the rationality of the given hypothesis. Hereafter, unless specified otherwise, we focus on the case  $D_f \rightarrow 0$  when referring to the secrecy outage probability  $\mathcal{P}_{so}$  of the typical FD Rx.

*Corollary 3:* In the small  $D_f$  regime, i.e.,  $D_f \rightarrow 0$ ,  $\mathcal{P}_{so}$  in (16) is approximated by

$$\mathcal{P}_{so} \approx 1 - \exp \left[ - \frac{\pi \lambda_e}{C_{\alpha,2} \lambda_f P_{tf}^\delta \beta_e^\delta} \left( N_e - 1 + \frac{1}{1 + P_{tf} \beta_e} \right) \right]. \quad (17)$$

<sup>5</sup>Successfully decoding multiplex signals actually depends on the so-called ‘capacity range’, which is extremely hard to analyze if we have more than two users. In this paper, we are not going to spend time to analyze the complicated multiplex channel capacity, instead we consider the eavesdropping capacity of successive interference cancellation, which is actually the worse case scenario.



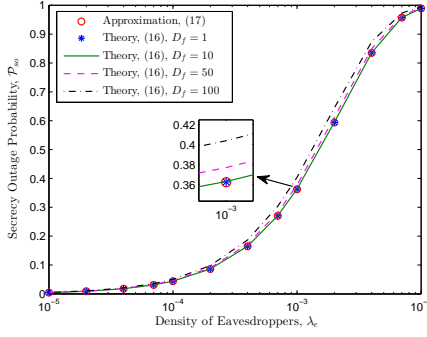


Fig. 3: Secrecy outage probability vs.  $\lambda_e$  for different values of  $D_f$ , with  $P_t = 10\text{dBm}$ ,  $N_t = 1$ ,  $N_e = 4$ ,  $\lambda_f = 10^{-3}$  and  $\beta_e = 1$ .

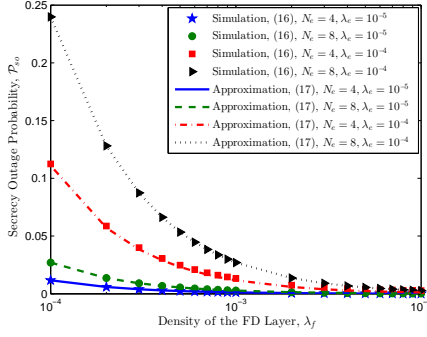


Fig. 4: Secrecy outage probability vs.  $\lambda_f$  for different values of  $N_e$  and  $\lambda_e$ , with  $P_t = 20\text{dBm}$ ,  $N_t = 1$  and  $\beta_e = 1$ .

*Proof:* Please see Appendix D. ■

Fig. 4 shows that the approximated values in (17) for the secrecy outage probability  $\mathcal{P}_{so}$  are quite close to the exact results of Monte-Carlo simulations. The value of  $\mathcal{P}_{so}$  gets larger as either the number  $N_e$  of eavesdropper's antennas or the density  $\lambda_e$  of eavesdroppers increases. To reduce the secrecy outage probability, we should better deploy more FD jammers, i.e., increasing the value of  $\lambda_f$ .

Although eavesdroppers do not collude with each other, they may use large antennas for better wiretapping. Considering that the value of  $N_e$  goes to infinity,  $\mathcal{P}_{so}$  in (17) reduces to

$$\mathcal{P}_{so} = 1 - \exp\left(-\frac{\pi\lambda_e N_e}{C_{\alpha,2}\lambda_f P_{tf}^\delta \beta_e^\delta}\right). \quad (18)$$

We observe from (18) that  $\mathcal{P}_{so}$  increases as  $\alpha$  increases. This is because, in an environment of a larger path loss, jamming signals have undergone stronger attenuation before they arrive at the eavesdroppers.

### C. Network-wide Secrecy Throughput

In this subsection, we investigate network-wide secrecy throughput  $\mathcal{T}_s$  under a connection probability  $\mathcal{P}_t(\beta_t) = \sigma$  and a secrecy outage constraint  $\mathcal{P}_{so}(\beta_e) = \epsilon$ , which is defined in (6). Clearly, if  $\beta_t^* \leq \beta_e^*$ , a positive  $\mathcal{T}_s$  that simultaneously satisfies the given probabilities does not exist, thus, transmissions should be suspended. Note that although increasing the density  $\lambda_f$  of the FD tier may increase network-wide secrecy throughput  $\mathcal{T}_s$ , it introduces greater interference to the HD tier,

thus reducing network-wide throughput  $\mathcal{T}_c$ . To achieve a good balance, we should carefully choose the value of  $\lambda_f$ . In the following, we aim to maximize  $\mathcal{T}_s$  by optimizing  $\lambda_f$  under a guarantee that  $\mathcal{T}_c$  lies above a target throughput  $T_c$ . This optimization problem is formulated as

$$\max_{\lambda_f} \mathcal{T}_s, \quad \text{s.t. } \mathcal{T}_c \geq T_c. \quad (19)$$

To proceed, we first calculate  $\beta_t^*$  and  $\beta_e^*$  from  $\mathcal{P}_t(\beta_t) = \sigma$  and  $\mathcal{P}_{so}(\beta_e) = \epsilon$ , respectively. In general, the analytical expressions of the exact  $\beta_t^*$  and  $\beta_e^*$  are unavailable due to the complexity of (9) and (16); we can only numerically calculate  $\beta_t^*$  and  $\beta_e^*$ , which makes solving problem (19) extremely difficult. To facilitate the analysis and provide useful insights into network design, we resort to some approximate results of the connection and secrecy outage probabilities. To ensure a high level of reliability, the connection probability  $\sigma$  is expected to be large, which allows us to use (12) to calculate  $\beta_t^*$ .

*Lemma 1:* In the large  $\sigma$  regime, i.e.,  $\sigma \rightarrow 1$ , the root  $\beta_t$  of the equation  $\mathcal{P}_t(\beta_t) = \sigma$  is given by

$$\beta_t^* = \left( \frac{1 - \sigma}{C_{\alpha,2} D_f^2 K_{\alpha, N_f - 2} \left( P_{hf}^\delta \lambda_h + (1 + P_{tf}^\delta) \lambda_f \right)} \right)^{\frac{\alpha}{2}}. \quad (20)$$

*Proof:* Recalling Corollary 1, we obtain (20) by solving the equation  $1 - \Lambda_{\beta_t}^L K_{\alpha, N_f - 2} = \sigma$ . ■

Considering the scenario of large-antenna eavesdroppers, i.e.,  $N_e \gg 1$ , we have the following lemma.

*Lemma 2:* In the large  $N_e$  regime, the root  $\beta_e$  of the equation  $\mathcal{P}_{so}(\beta_e) = \epsilon$  is given by

$$\beta_e^* = \frac{1}{P_{tf}} \left( \frac{\pi \lambda_e N_e}{C_{\alpha,2} \lambda_f \ln \frac{1}{1-\epsilon}} \right)^{\frac{\alpha}{2}}. \quad (21)$$

*Proof:* Recalling (18), we obtain (21) by solving the equation  $1 - e^{-\pi \lambda_e N_e / (C_{\alpha,2} \lambda_f P_{tf}^\delta \beta_e^\delta)} = \epsilon$ . ■

Having obtained  $\beta_t^*$  in (20) and  $\beta_e^*$  in (21), we begin to solve problem (19). Since we focus on variable  $\lambda_f$ , we substitute (6) into (19), and reform problem (19) as follows by introducing an auxiliary function  $F(\lambda_f)$  which shows explicitly the relationship between objective function  $\mathcal{T}_s$  and  $\lambda_f$ ,

$$\max_{\lambda_f} \mathcal{T}_s = \frac{\sigma}{\ln 2} [F(\lambda_f)]^+, \quad \text{s.t. } 0 < \lambda_f \leq \lambda_f^U, \quad (22)$$

where  $F(\lambda_f) = \lambda_f \ln \frac{1 + X(1 + Y\lambda_f)^{-\alpha/2}}{1 + Z\lambda_f^{-\alpha/2}}$ ,  $\lambda_f^U \triangleq \frac{(1 - \sigma_c) / (C_{\alpha,2} D_h^2 K_{\alpha, N_h}) (2^{T_c / (\lambda_h \sigma_c)} - 1)^{-\delta} - \lambda_h}{P_{th}^\delta + P_{fh}^\delta}$  is obtained from  $\mathcal{T}_c = \lambda_h \sigma_c \log(1 + \beta_c^*) = T_c$  in (19), and  $X \triangleq \left( \frac{1 - \sigma}{C_{\alpha,2} D_f^2 K_{\alpha, N_f - 2} P_{hf}^\delta \lambda_h} \right)^{\alpha/2}$ ,  $Y \triangleq \frac{1 + P_{tf}^\delta}{P_{hf}^\delta \lambda_h}$  and  $Z \triangleq \frac{1}{P_{tf}} \left( \frac{\pi \lambda_e N_e}{C_{\alpha,2} \ln \frac{1}{1-\epsilon}} \right)^{\alpha/2}$ . To achieve a positive  $\mathcal{T}_s$  in (22),  $F(\lambda_f) > 0$ , i.e.,  $X(1 + Y\lambda_f)^{-\alpha/2} > Z\lambda_f^{-\alpha/2}$  must be guaranteed, and thus we have  $\lambda_f > \lambda_f^L \triangleq 1 / ((X/Z)^\delta - Y)$

and  $(X/Z) > Y^{\frac{\alpha}{2}}$ , which further yield

$$(1 - \sigma) \ln \frac{1}{1 - \epsilon} > \pi \lambda_e N_e D_f^2 K_{\alpha, N_f - 2} \left(1 + P_{tf}^{-\delta}\right). \quad (23)$$

That is to say, a large  $\sigma$  and a small  $\epsilon$  might not be simultaneously promised. In the following, we consider the case that a positive  $\mathcal{T}_s$  exists, i.e.,  $\lambda_f > \lambda_f^L$ . Thereby, problem (22) is equivalent to

$$\max_{\lambda_f} F(\lambda_f), \quad \text{s.t. } \lambda_f^L < \lambda_f \leq \lambda_f^U. \quad (24)$$

In the following theorem, we can prove the *quasi-concavity* [38, Sec. 3.4.2] of  $F(\lambda_f)$  w.r.t.  $\lambda_f$  in the range  $(\lambda_f^L, \infty)$ , and derive the optimal  $\lambda_f$  that maximizes  $F(\lambda_f)$  (or  $\mathcal{T}_s$ ).

**Theorem 4:** The optimal density  $\lambda_f$  that maximizes network-wide secrecy throughput  $\mathcal{T}_s$  is

$$\lambda_f^* = \begin{cases} \min(\lambda^*, \lambda_f^U), & (X/Z) > Y^{\frac{\alpha}{2}} \text{ and } \lambda_f^L \leq \lambda_f^U, \\ \emptyset, & \text{otherwise,} \end{cases} \quad (25)$$

where  $\lambda^*$  is the unique root of the following equation,

$$\ln \frac{f_1(\lambda)}{f_2(\lambda)} + \frac{\frac{\alpha}{2} f_1(\lambda) [f_2(\lambda) - 1] - \frac{\alpha}{2} \lambda [f_1(\lambda) - f_2(\lambda)] Y}{f_1(\lambda) f_2(\lambda) (1 + \lambda Y)} = 0, \quad (26)$$

with  $f_1(\lambda) = 1 + X(1 + Y\lambda)^{-\frac{\alpha}{2}}$  and  $f_2(\lambda) = 1 + Z\lambda^{-\frac{\alpha}{2}}$ . The left-hand side (LHS) of (26) is first positive and then negative; thus, the value of  $\lambda^*$  can be efficiently calculated using the bisection method. Here,  $\lambda_f^* = \emptyset$  means no  $\lambda_f$  can produce a positive  $\mathcal{T}_s$  under a given pair  $(\sigma, \epsilon)$ .

*Proof:* Please see Appendix E. ■

Theorem 4 indicates that by properly choosing the value of  $\lambda_f$ , we can achieve the maximum network-wide secrecy throughput for the FD tier while guaranteeing a minimum required network-wide throughput for the HD tier. Substituting the optimal  $\lambda_f^*$  into (22) yields the maximum  $\mathcal{T}_s^*$ , which is shown in Fig. 5. Just as analyzed previously, only those  $\sigma$  and  $\epsilon$  that satisfy (23) can yield a positive  $\mathcal{T}_s^*$ . While  $\mathcal{T}_s^*$  increases in  $\epsilon$ ,  $\mathcal{T}_s^*$  initially increases in  $\sigma$  and then decreases in it. The underlying reason is, too small a  $\sigma$  corresponds to a small probability of successful transmission, whereas too large a  $\sigma$  limits the transmission rate; either aspect results in a small  $\mathcal{T}_s^*$ , as can be seen from (6).

In addition to the density of the FD tier  $\lambda_f$ , the jamming power of the FD Rx  $P_t$ <sup>6</sup> also triggers a non-trivial tradeoff between transmission reliability and secrecy, thus impacting network-wide secrecy throughput  $\mathcal{T}_s$ . Similar to Theorem 4, we can also prove the quasi-concavity of  $\mathcal{T}_s$  on  $P_t$ , which is validated in Fig. 6. We observe that, in a certain range of  $\lambda_f$ , how  $\mathcal{T}_s$  varies w.r.t.  $\lambda_f$  heavily depends on the value of  $P_t$ . For example, if at the small  $P_t$  regime  $\mathcal{T}_s$  increases in  $\lambda_f$ ,  $\mathcal{T}_s$  might decrease in  $\lambda_f$  in the large  $P_t$  regime.

#### IV. MULTI-ANTENNA-JAMMING FD RECEIVER

In this section, we consider the scenario of the FD Rx using multi-antenna jamming. Thanks to the extra degrees of freedom provided by multiple jamming antennas, each FD Rx

<sup>6</sup>Since we only focus on the optimization of network density, the power control issue is outside the scope of this paper.

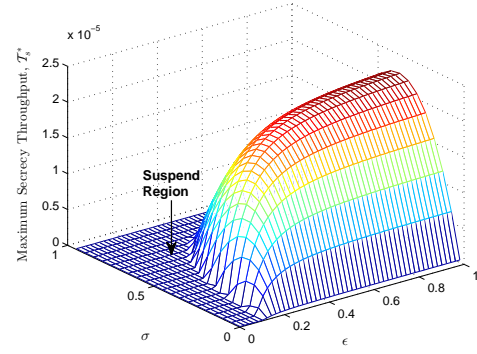


Fig. 5: Maximum network-wide secrecy throughput vs.  $\sigma$  and  $\epsilon$ , with  $P_t = 20\text{dBm}$ ,  $N_f = 4$ ,  $N_t = 1$ ,  $N_e = 8$ ,  $\lambda_e = 10^{-2}$ ,  $\sigma_c = 0.9$  and  $T_c = 10^{-3}$ . In the dark blue areas, there is no positive  $\mathcal{T}_s$  that simultaneously satisfies connection and secrecy outage probabilities.

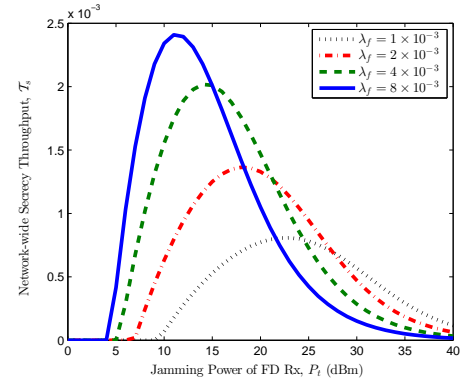


Fig. 6: Network-wide secrecy throughput vs.  $P_t$  for different values of  $\lambda_f$  with  $N_f = 4$ ,  $N_t = 1$ ,  $N_e = 4$ ,  $\lambda_e = 10^{-3}$ ,  $\sigma = 0.9$ ,  $\sigma_c = 0.9$ ,  $\epsilon = 0.1$  and  $T_c = 10^{-3}$ .

is able to inject jamming signals into the null space of the SI channel such that SI will not leak out to the Rx's input, and MRC reception can be simply adopted at the input for the desired signal. This is inspired by the idea of the artificial noise scheme proposed in [17]. We will see the analysis of multi-antenna jamming is much more different from and much more sophisticated than that of single-antenna jamming.

Without loss of generality, we consider a typical FD Rx at the origin  $o$ . The details of SSIC are given as follows. We first use MRC reception at the input of the typical FD Rx, the weight vector of which can be obtained from (1), i.e.,  $\tilde{\mathbf{w}}_f = \frac{\mathbf{f}_{fo}^H}{\|\mathbf{f}_{fo}\|}$ . Here we use superscript  $\sim$  to distinguish the multi-antenna jamming case from the single-antenna jamming case. We then design the jamming signal  $\mathbf{v}_o$  in (1) in the form of  $\mathbf{v}_o = \tilde{\mathbf{F}}_o \tilde{\mathbf{v}}_o$ , where  $\tilde{\mathbf{v}}_o \in \mathbb{C}^{N_j \times 1}$  is an  $N_j$ -stream jamming signal vector with i.i.d. entries  $\tilde{v}_i \sim \mathcal{CN}(0, 1/N_j)$  and  $N_j \leq N_t - 1$ ,  $\tilde{\mathbf{F}}_o \in \mathbb{C}^{N_t \times N_j}$  is the projection matrix onto the null space of vector  $(\tilde{\mathbf{w}}_f \mathbf{F}_{oo})^H$  such that the columns of  $\left[ \frac{(\tilde{\mathbf{w}}_f \mathbf{F}_{oo})^H}{\|\tilde{\mathbf{w}}_f \mathbf{F}_{oo}\|}, \tilde{\mathbf{F}}_o \right]$  constitute an orthogonal basis, i.e.,  $\tilde{\mathbf{w}}_f \mathbf{F}_{oo} \mathbf{v}_o = 0$ . In this way, SI is completely eliminated in the spatial domain. It is worth mentioning that,  $\tilde{\mathbf{v}}_o$  includes but is not limited to an  $N_t - 1$ -stream signal vector. Although  $N_t - 1$ -dimension null space should better be injected with jamming signals to confuse eavesdroppers in a point-to-point



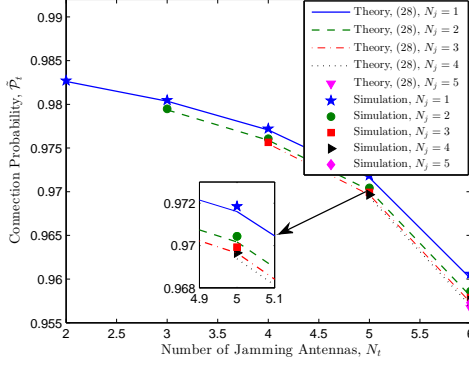


Fig. 7: Connection probability vs.  $N_t$  for different values of  $N_j$ , with  $P_t = 20\text{dBm}$ ,  $N_f = 8$ ,  $\lambda_f = 10^{-3}$  and  $\beta_t = 1$ .

transmission [17], there is no general conclusion from the network perspective, since jamming signals impair not only eavesdroppers but also legitimate users.

#### A. Connection Probability

From the above discussion, the SIR of the typical FD Rx can be obtained from (1), which is

$$\widetilde{\text{SIR}}_f = \frac{P_f \|\mathbf{f}_{\hat{o}o}\|^2 D_f^{-\alpha}}{\tilde{I}_h + \tilde{I}_f}, \quad (27)$$

where  $\tilde{I}_h \triangleq \sum_{\hat{z} \in \hat{\Phi}_h} P_h |\tilde{\mathbf{w}}_f \mathbf{f}_{\hat{z}o}|^2 D_{\hat{z}o}^{-\alpha}$  and  $\tilde{I}_f \triangleq \sum_{\hat{z} \in \hat{\Phi}_f \setminus o} (P_f |\tilde{\mathbf{w}}_f \mathbf{f}_{\hat{z}o}|^2 D_{\hat{z}o}^{-\alpha} + (P_t/N_j) \|\tilde{\mathbf{w}}_f \mathbf{F}_{zo} \tilde{\mathbf{F}}_z\|^2 D_{zo}^{-\alpha})$  are the aggregate interferences from the HD and FD tiers, respectively. Substituting (27) into (4) produces the connection probability of the typical FD Rx, denoted by  $\tilde{P}_t$ . As discussed in the single-antenna jamming case, the exact expression of  $\tilde{P}_t$  can be derived, which however is not in an analytical form. Instead, we provide a more tractable lower bound for  $\tilde{P}_t$  in the following theorem.

**Theorem 5:** The connection probability  $\tilde{P}_t$  of the typical FD Rx is lower bounded by

$$\tilde{P}_t^L = e^{-\tilde{\Lambda}_f^L \beta_t^\delta} \left( 1 + \sum_{m=1}^{N_f - N_t - 1} \frac{1}{m!} \sum_{n=1}^m (\delta \tilde{\Lambda}_f^L \beta_t^\delta)^n \Upsilon_{m,n} \right), \quad (28)$$

where  $\tilde{\Lambda}_f^L \triangleq C_{\alpha,2} P_{hf}^\delta \lambda_h D_f^2 + C_{\alpha,2} \lambda_f D_f^2 + C_{\alpha,N_j+1} (P_{tf}/N_j)^\delta \lambda_f D_f^2$  and  $\Upsilon_{m,n}$  has been defined in (11).

*Proof:* Please see Appendix F. ■

To further facilitate the analysis, an approximation for  $\tilde{P}_t$  is provided by the following corollary.

**Corollary 4:** In the large probability region, i.e.,  $\tilde{P}_t \rightarrow 1$ ,  $\tilde{P}_t$  is approximated by

$$\tilde{P}_t \approx 1 - \tilde{\Lambda}_f \beta_t^\delta K_{\alpha,N_f - N_t}, \quad (29)$$

where  $\tilde{\Lambda}_f = \tilde{\Lambda}_f^L$  and  $K_{\alpha,N}$  has been defined in Corollary 1.

Fig. 7 shows that the result in (29) approximates to the exact connection probability  $\tilde{P}_t$  provided by Monte-Carlo simulations. We see that  $\tilde{P}_t$  greatly reduces as the number

$N_t$  of jamming antennas increases. In addition,  $\tilde{P}_t$  suffers a slight decrease when the number  $N_j$  of jamming signal streams increases. This implies when the value of  $N_t$  is fixed,  $\tilde{P}_t$  is less insensitive to the value of  $N_j$ .

Following similar steps in Theorem 5 and Corollary 4, an approximation for the connection probability  $\tilde{P}_c$  of a typical HD Rx in the large probability region is given in the following corollary.

**Corollary 5:** Define  $\tilde{\Lambda}_h = C_{\alpha,2} \lambda_h D_h^2 + C_{\alpha,2} P_{fh}^\delta \lambda_f D_h^2 + C_{\alpha,N_j+1} (P_{th}/N_j)^\delta \lambda_f D_h^2$ . In the large probability region, i.e.,  $\tilde{P}_c \rightarrow 1$ , the connection probability  $\tilde{P}_c$  of a typical HD Rx is approximated by

$$\tilde{P}_c \approx 1 - \tilde{\Lambda}_h \beta_c^\delta K_{\alpha,N_h}. \quad (30)$$

#### B. Secrecy Outage Probability

Assuming that every eavesdropper has the capability of multiuser decoding and uses the MMSE receiver, the weight vector of the eavesdropper located at  $e$  can be obtained from (3), which is

$$\tilde{\mathbf{w}}_e = \tilde{\mathbf{R}}_e^{-1} \mathbf{g}_{oe}, \quad (31)$$

where  $\tilde{\mathbf{R}}_e \triangleq (P_t/N_j) \mathbf{G}_{oe} \tilde{\mathbf{F}}_o \tilde{\mathbf{F}}_o^H \mathbf{G}_{oe}^H D_{oe}^{-\alpha} + \sum_{z \in \Phi_f \setminus o} (P_t/N_j) \mathbf{G}_{ze} \tilde{\mathbf{F}}_z \tilde{\mathbf{F}}_z^H \mathbf{G}_{ze}^H D_{ze}^{-\alpha}$ ; the resulting SIR is

$$\widetilde{\text{SIR}}_e = P_f \mathbf{g}_{oe}^H \tilde{\mathbf{R}}_e^{-1} \mathbf{g}_{oe} D_{oe}^{-\alpha}. \quad (32)$$

Due to the existence of multi-stream jamming signals, computing secrecy outage probability requires using the integer partitions of a positive integer [34]. For convenience, we describe the integer partitions of a positive integer  $k$  by introducing an integer partition matrix  $\Theta_k$ . For example, the integer partitions of 4 is characterized by

$$\Theta_4 = \begin{bmatrix} 4 & & & & \\ 3 & 1 & & & \\ 2 & 2 & & & \\ 2 & 1 & 1 & & \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \quad (33)$$

In the following, we denote  $|\xi_k|$  as the number of rows of  $\Theta_k$ , and  $\xi_{i,j,k}$ ,  $|\xi_{j,k}|$ ,  $\phi_{i,j,k}$  and  $|\phi_{j,k}|$  as the  $i$ -th entry, the number of entries, the number of the  $i$ -th largest entry and the number of non-repeated entries in the  $j$ -th row of  $\Theta_k$ , respectively. We provide a closed-form expression for secrecy outage probability  $\tilde{P}_{so}$  in the following theorem.

**Theorem 6:** The secrecy outage probability of a typical multi-antenna jamming FD Rx is

$$\tilde{P}_{so} = 1 - \exp \left( - \frac{\pi \lambda_e}{C_{\alpha,N_j+1} \lambda_f} \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,N_j)} \binom{N_j}{i} \times \frac{(P_{tf} \beta_e / N_j)^{i-\delta}}{(1 + P_{tf} \beta_e / N_j)^{N_j}} \sum_{j=1}^{|\xi_{n-i}|} (-1)^{|\xi_{j,n-i}|} |\xi_{j,n-i}|! \Xi_{j,n-i} \right), \quad (34)$$

where  $\Xi_{j,n} = \frac{\prod_{m=1}^{|\xi_{j,n}|} \prod_{k=1}^{\xi_{m,j,n}} \frac{(N_j+1-k)(k-1-\delta)}{k(N_j-k+\delta)}}{\prod_{i=1}^{|\phi_{j,n}|} \phi_{i,j,n}!}$ . Here, we let  $|\xi_0| = 1$ ,  $|\xi_{j,0}| = 0$  and  $\Xi_{j,0} = 1$ .

*Proof:* Please see Appendix G. ■

We see that secrecy outage probability  $\tilde{P}_{so}$  is affected by the number  $N_j$  of jamming signal streams rather than the

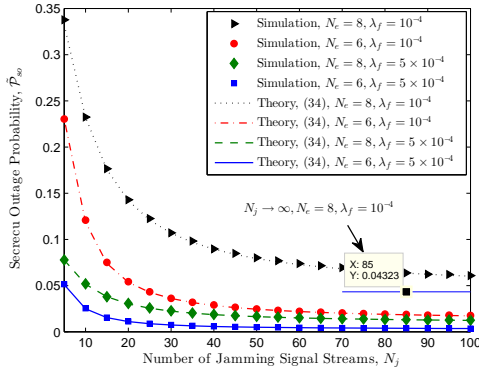


Fig. 8: Secrecy outage probability vs.  $N_j$  for different values of  $N_e$  and  $\lambda_f$ , with  $P_t = 10\text{dBm}$ ,  $\lambda_e = 10^{-4}$  and  $\beta_e = 1$ .

number  $N_t$  of jamming antennas. The result in (34) is well verified by Monte-Carlo simulations, just as shown in Fig. 8. To better understand the effect of  $N_j$  on  $\tilde{P}_{so}$ , we investigate the asymptotic behavior of  $\tilde{P}_{so}$  w.r.t.  $N_j$  by considering the cases  $N_j = 1$  and  $N_j \rightarrow \infty$ , respectively.

*Corollary 6:* When  $N_j = 1$ ,  $\tilde{P}_{so}$  in (34) shares the same expression as the one given in (17).

*Proof:* Substituting  $N_j = 1$  into  $\Xi_{j,n-i}$ , we have  $\Xi_{j,n-i} = 0$  for  $j < |\xi_{n-i}|$ . Since the  $|\xi_{n-i}|$ -th integer partition of  $n-i$  (i.e., the last row of  $\Theta_{n-i}$ ) must be  $n-i$  ones, we have  $|\phi_{|\xi_{n-i}|,n-i}| = 1$  and  $|\xi_{|\xi_{n-i}|,n-i}| = \phi_{1,|\xi_{n-i}|,n-i}$ . Therefore, the term  $\sum_{j=1}^{|\xi_{n-i}|} (-1)^{|\xi_{j,n-i}|} |\xi_{j,n-i}|! \Xi_{j,n-i}$  in (34) reduces to  $(-1)^{|\xi_{|\xi_{n-i}|,n-i}|} |\xi_{|\xi_{n-i}|,n-i}|! \Xi_{|\xi_{n-i}|,n-i} = 1$ , substituting which into (34) completes the proof. ■

Corollary 6 implies emitting a single-stream jamming signal using multiple antennas has the same effect as single-antenna jamming in confounding eavesdroppers.

*Corollary 7:* As  $N_j \rightarrow \infty$ ,  $\tilde{P}_{so}$  in (34) tends to the following constant value

$$1 - \exp \left( - \frac{\lambda_e}{\Gamma(1-\delta)\lambda_f} \sum_{n=0}^{N_e-1} \sum_{i=0}^n \frac{e^{-P_{tf}\beta_e}}{i!(P_{tf}\beta_e)^{\delta-i}} \times \sum_{j=1}^{|\xi_{n-i}|} \frac{|\xi_{j,n-i}|! \prod_{m=1}^{|\xi_{j,n-i}|} \prod_{k=1}^{\xi_{m,j,n-i}} \frac{k-1-\delta}{k}}{(-1)^{|\xi_{j,n-i}|} \prod_{i=1}^{|\phi_{j,n-i}|} \phi_{i,j,n-i}!} \right). \quad (35)$$

*Proof:* Invoking  $\lim_{N \rightarrow \infty} \frac{\Gamma(N+\delta)}{\Gamma(N)N^\delta} = 1$  and  $\lim_{N \rightarrow \infty} (1 + \frac{x}{N})^N = e^x$  in (34) directly yields (35). ■

Corollary 7 implies increasing jamming signal streams can not arbitrarily reduce secrecy outage probability, just as validated in Fig. 8. This is because the total power  $P_t$  of jamming signals is limited. Conversely, if  $P_t$  in (35) goes to infinity,  $\tilde{P}_{so}$  reduces to zero.

### C. Network-wide Secrecy Throughput

The network-wide secrecy throughput  $\tilde{T}_s$  in multi-antenna jamming scenario under a connection probability  $\tilde{P}_t(\beta_t) = \sigma$  and a secrecy outage probability  $\tilde{P}_{so}(\beta_e) = \epsilon$  has the same form as (6). We aim to optimize  $\lambda_f$  to maximize  $\tilde{T}_s$  while guaranteeing a certain level of the HD tier throughput, i.e.,

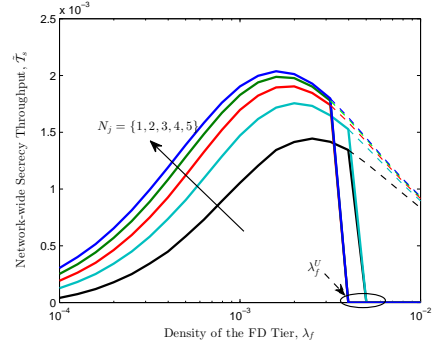


Fig. 9: Network-wide secrecy throughput vs.  $\lambda_f$  for different values of  $N_j$ , with  $P_t = 20\text{dBm}$ ,  $N_f = N_e = 8$ ,  $N_t = 6$ ,  $\lambda_e = 10^{-4}$ ,  $\sigma = \sigma_c = 0.9$ ,  $\epsilon = 0.02$  and  $T_c = 10^{-3}$ . The dashed lines show the values of  $\tilde{T}_s$  without an HD tier throughput constraint, i.e.  $T_c = 0$ .

$\tilde{T}_c \geq T_c$ , with  $\tilde{T}_c$  sharing the form of  $T_c$  given in Sec. II-A. Before proceeding to the optimization problem, we compute  $\beta_t^*$  and  $\beta_e^*$  from the equations  $\tilde{P}_t(\beta_t) = \sigma$  and  $\tilde{P}_{so}(\beta_e) = \epsilon$ , respectively.

*Proposition 1:* In the large probability region, i.e.,  $\sigma \rightarrow 1$ , the root of  $\tilde{P}_t(\beta_t) = \sigma$  is given by

$$\beta_t^* = \left( \frac{(1-\sigma) / (C_{\alpha,2} D_f^2 K_{\alpha,N_f-N_t})}{P_{hf}^\delta \lambda_h + \left( 1 + \frac{C_{\alpha,N_f+1}}{C_{\alpha,2}} \left( \frac{P_{tf}}{N_j} \right)^\delta \right) \lambda_f} \right)^{\alpha/2}. \quad (36)$$

*Proof:* Recalling Corollary 4, (36) is obtained by solving  $1 - \tilde{\lambda}_f \beta_t^\delta K_{\alpha,N_f-N_t} = \sigma$ . ■

Generally, it is impossible to derive a closed-form expression for  $\beta_e^*$  due to the complicated integer partitions in (34). However, an analytical approximation for  $\beta_e^*$  can be readily obtained from (17) by considering the single jamming signal stream, i.e.,  $N_j = 1$ , in the large-antenna eavesdropper case.

*Proposition 2:* When  $N_e \gg 1$  and  $N_j = 1$ ,  $\beta_e$  that satisfies  $\tilde{P}_{so}(\beta_e) = \epsilon$  has the same expression as the one given in (21).

For the more general case  $N_j \geq 2$ , the value of  $\beta_e^*$  can be obtained via numerical calculation, i.e.,  $\beta_e^* = \tilde{P}_{so}^{-1}(\epsilon)$ , where  $\tilde{P}_{so}^{-1}(\epsilon)$  is the inverse function of  $\tilde{P}_{so}(\beta_e)$ .

In Fig. 9, we illustrate some numerical examples of network-wide secrecy throughput  $\tilde{T}_s$ . We see that  $\tilde{T}_s$  first increases and then decreases as the FD tier density  $\lambda_f$  increases. The value of  $\lambda_f$  should be properly chosen in order to maximize  $\tilde{T}_s$ . We also find that,  $\tilde{T}_s$  improves as the number  $N_j$  of jamming signal streams increases on the premise of a fixed number  $N_t$  of jamming antennas.

Next, we formulate the problem of maximizing network-wide secrecy throughput  $\tilde{T}_s$  as follows,

$$\max_{\lambda_f} \tilde{T}_s = \frac{\lambda_f \sigma}{\ln 2} \left[ \ln \frac{1 + \tilde{X}(1 + \tilde{Y}\lambda_f)^{-\alpha/2}}{1 + \tilde{P}_{so}^{-1}(\epsilon)} \right]^+, \quad (37a)$$

$$\text{s.t. } 0 < \lambda_f \leq \tilde{\lambda}_f^U, \quad (37b)$$

where  $\tilde{\lambda}_f^U \triangleq \frac{(1-\sigma_c)/(D_h^2 K_{\alpha,N_h})(2^{T_c/(\lambda_h \sigma_c)} - 1)^{-\delta} - C_{\alpha,2} \lambda_h}{C_{\alpha,2} P_{fh}^\delta + C_{\alpha,N_f+1}(P_{th}/N_j)^\delta}$  is obtained from  $\tilde{T}_c = T_c$ ,  $\tilde{X} \triangleq \left( \frac{1-\sigma}{C_{\alpha,2} D_f^2 K_{\alpha,N_f-N_t} P_{hf}^\delta \lambda_h} \right)^{\alpha/2}$  and

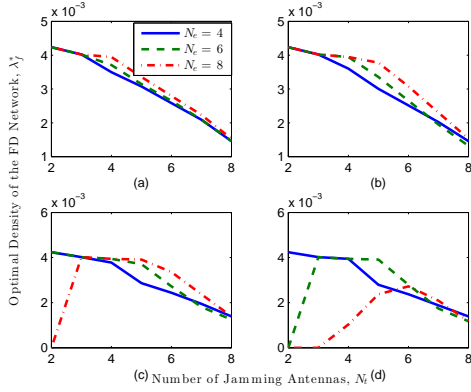


Fig. 10: Optimal density of the FD tier vs.  $N_t$  for different values of  $N_e$  and (a)  $\lambda_e = 2 \times 10^{-4}$ , (b)  $\lambda_e = 4 \times 10^{-4}$ , (c)  $\lambda_e = 7 \times 10^{-4}$ , (d)  $\lambda_e = 10^{-3}$ , with  $P_t = 20\text{dBm}$ ,  $N_f = 8$ ,  $N_j = N_t - 1$ ,  $\lambda_f = 2 \times 10^{-3}$ ,  $\sigma = \sigma_c = 0.9$ ,  $\epsilon = 0.02$  and  $T_c = 10^{-3}$ . Note that  $\lambda_f^* = 0$  when  $N_t = 2$  in (c) and  $N_t = 2, 3$  in (d). This means a positive secrecy throughput that simultaneously satisfies the connection and secrecy outage probability constraints can not be achieved, regardless of the value of  $\lambda_f$ .

$$\tilde{Y} \triangleq \frac{C_{\alpha,2} + C_{\alpha,N_j+1}(P_{t,f}/N_j)^\delta}{C_{\alpha,2} P_{h,f}^\delta \lambda_h}.$$

For the single jamming signal stream case  $N_j = 1$ ,  $\tilde{\mathcal{P}}_{so}^{-1}(\epsilon)$  has a closed-form expression given in (21), i.e.,  $\tilde{\mathcal{P}}_{so}^{-1}(\epsilon) = \beta_e^* = \tilde{Z} \lambda_f^{-\frac{\alpha}{2}}$  with  $\tilde{Z} \triangleq \frac{1}{P_{t,f}} \left( \frac{\pi \lambda_e N_e}{C_{\alpha,2} \ln \frac{1}{1-\epsilon}} \right)^{\frac{\alpha}{2}}$ . Accordingly, problem (37a) has the same form as problem (24). As a consequence, the optimal  $\lambda_f$  that maximizes  $\tilde{T}_s$  also shares the same form as (25), simply with  $X, Y, Z$  and  $\lambda_f^U$  replaced by  $\tilde{X}, \tilde{Y}, \tilde{Z}$  and  $\tilde{\lambda}_f^U$ , respectively.

For the more general case  $N_j \geq 2$ , we can only solve problem (37a) using one-dimension exhaustive search in the range  $(0, \tilde{\lambda}_f^U]$ . Since increasing the number  $N_j$  of jamming signal streams always benefits network-wide secrecy throughput, we should set  $N_j = N_t - 1$ . Thus,  $N_t - 1$ -dimension null space is fully injected with jamming signals. In Fig. 10 and Fig. 11, we illustrate the optimal density  $\lambda_f^*$  and the corresponding maximum network-wide secrecy throughput  $\tilde{T}_s^*$ , respectively.

From Fig. 10, we observe a general trend that the value of  $\lambda_f^*$  decreases as  $N_t$  increases on the premise of the existence of a positive  $\tilde{T}_s^*$ . The reason behind is twofold: on one hand, adding jamming antennas provides relief to deploying more FD jammers to degrade the wiretap channels; on the other hand, reducing the number of FD Tx-Rx pairs reduces network interference, thus improving the main channels. How the value of  $\lambda_f^*$  is influenced by  $N_e$  depends on the specific values of  $\lambda_e$  and  $N_t$ . For example, if each eavesdropper adds receive antennas, more FD jammers are needed for a relatively small  $N_t$  or a small  $\lambda_e$  (see (a), (b) and (c)), whereas fewer FD jammers might be better as  $N_t$  or  $\lambda_e$  goes large (see  $N_t = 7$  in (c) and  $N_t = 5$  in (d)). This is because, if we continue to add FD jammers, we can scarcely achieve a positive secrecy throughput.

In Fig. 11, we see that the maximum network-wide secrecy throughput  $\tilde{T}_s^*$  always deteriorates as  $\lambda_e$  or  $N_e$  increases. How the value of  $\tilde{T}_s^*$  is affected by  $N_t$  depends on the specific values of  $\lambda_e$  and  $N_e$ . Specifically, for relatively small values of  $\lambda_e$  and  $N_e$ ,  $\tilde{T}_s^*$  decreases as  $N_t$  increases (see (a)). This

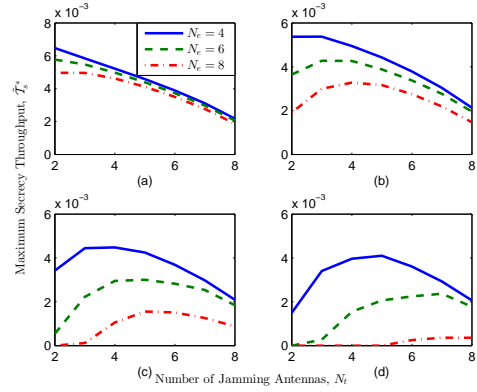


Fig. 11: Maximum network-wide secrecy throughput vs.  $N_t$  for different values of  $N_e$  and (a)  $\lambda_e = 2 \times 10^{-4}$ , (b)  $\lambda_e = 4 \times 10^{-4}$ , (c)  $\lambda_e = 7 \times 10^{-4}$ , (d)  $\lambda_e = 10^{-3}$ , with  $P_t = 20\text{dBm}$ ,  $N_f = 8$ ,  $N_j = N_t - 1$ ,  $\lambda_f = 2 \times 10^{-3}$ ,  $\sigma = \sigma_c = 0.9$ ,  $\epsilon = 0.02$  and  $T_c = 10^{-3}$ .

means we should use as few jamming antennas as possible. However, as  $\lambda_e$  or  $N_e$  increases,  $\tilde{T}_s^*$  first increases and then decreases as  $N_t$  increases (see (b), (c) and (d)). This implies that a modest value of  $N_t$  is required to balance improving the main channels with degrading the wiretap channels.

## V. CONCLUSIONS

This paper comprehensively studies physical-layer security using FD Rx jamming techniques against randomly located eavesdropper in a heterogeneous DWN consisting of both HD and FD tiers. The connection probability and the secrecy outage probability of a typical FD Rx is analyzed for single- and multi-antenna jamming scenarios, and the optimal FD tier density is provided for maximizing network-wide secrecy throughput under constraints including the given dual probabilities and the network-wide throughput of the HD tier. Numerical results are presented to validate our theoretical analysis, and show the benefits of FD Rx jamming in improving network-wide secrecy throughput.

## APPENDIX

### A. Proof of Theorem 1

Let  $s \triangleq D_f^\alpha \beta_t / P_f$  and  $I_o = I_h + I_f$ .  $\mathcal{P}_t$  can be calculated by substituting (8) into (4)

$$\begin{aligned} \mathcal{P}_t &= \mathbb{E}_{I_o} [\mathbb{P} \{ \|\mathbf{f}_{oo}^H \mathbf{U}\|^2 \geq s I_o \}] \stackrel{(a)}{=} \mathbb{E}_{I_o} \left[ e^{-s I_o} \sum_{m=0}^{N_f-3} \frac{s^m I_o^m}{m!} \right] \\ &= \sum_{m=0}^{N_f-3} \mathbb{E}_{I_o} \left[ \frac{s^m e^{-s I_o}}{m!} I_o^m \right] \stackrel{(b)}{=} \sum_{m=0}^{N_f-3} \left[ \frac{s^m \mathcal{L}_{I_o}^{(m)}(s)}{(-1)^m m!} \right], \end{aligned} \quad (38)$$

where (a) holds for  $\|\mathbf{f}_{oo}^H \mathbf{U}\|^2 \sim \Gamma(N_f - 2, 1)$ , and (b) is obtained from [32, Theorem 1]. Due to the independence of  $I_h$  and  $I_f$ ,  $\mathcal{L}_{I_o}(s)$  is given by

$$\mathcal{L}_{I_o}(s) = \mathbb{E}_{I_o} [e^{-s I_o}] = \mathcal{L}_{I_h}(s) \mathcal{L}_{I_f}(s). \quad (39)$$

$\mathcal{L}_{I_h}(s)$  can be directly obtained from [11, (8)], which is

$$\mathcal{L}_{I_h}(s) = \exp(-\lambda_h C_{\alpha,2} (P_h s)^\delta). \quad (40)$$

$\mathcal{L}_{I_f}(s) = \mathbb{E}_{I_f} [e^{-sI_f}]$  can be computed as

$$\mathcal{L}_{I_f}(s) = \mathbb{E}_{\hat{\Phi}_f} \left[ \prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} e^{-s \left( \frac{P_f |\mathbf{w}_f \mathbf{f}_{\hat{z}o}|^2}{D_{\hat{z}o}^\alpha} + \frac{P_t |\mathbf{w}_f \mathbf{f}_{zo}|^2}{D_{zo}^\alpha} \right)} \right] \quad (41)$$

$$\stackrel{(c)}{=} \mathbb{E}_{\hat{\Phi}_f} \left[ \prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} \frac{1}{1 + P_f s D_{\hat{z}o}^{-\alpha}} \frac{1}{1 + P_t s D_{zo}^{-\alpha}} \right] \quad (42)$$

$$\stackrel{(d)}{=} \exp \left( -\lambda_f \int_0^\infty \int_0^{2\pi} \left( 1 - \frac{1}{1 + P_f s r^{-\alpha}} \times \frac{1}{1 + P_t s \left( r^2 + D_f^2 - 2rD_f \cos \theta \right)^{-\alpha/2}} \right) r d\theta dr \right), \quad (43)$$

where (c) holds for  $|\mathbf{w}_f \mathbf{f}_{\hat{z}o}|^2, |\mathbf{w}_f \mathbf{f}_{zo}|^2 \sim \text{Exp}(1)$ , and (d) is derived by using the probability generating functional (PGFL) over a PPP [36]. Substituting (40) and (43) into (39) completes the proof.

### B. Proof of Theorem 2

To provide a lower bound for  $\mathcal{P}_t$ , we need only provide a lower bound for  $\mathcal{L}_{I_f}(s)$ . This is because, a lower bound for  $\mathcal{L}_{I_f}(s)$  actually overestimates the aggregate interference  $I_f$  from the FD tier, which leads to a lower bound for  $\mathcal{P}_t$ . From (41), we have

$$\begin{aligned} \mathcal{L}_{I_f}(s) &\stackrel{(e)}{\geq} \mathbb{E}_{\hat{\Phi}_f} \left[ \prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} e^{-\frac{s P_f |\mathbf{w}_f \mathbf{f}_{\hat{z}o}|^2}{D_{\hat{z}o}^\alpha}} \right] \mathbb{E}_{\Phi_f \setminus o} \left[ \prod_{z \in \Phi_f \setminus o} e^{-\frac{s P_t |\mathbf{w}_f \mathbf{f}_{zo}|^2}{D_{zo}^\alpha}} \right] \\ &\stackrel{(f)}{=} e^{-\lambda_f C_{\alpha,2} (P_f s)^\delta} e^{-\lambda_f C_{\alpha,2} (P_t s)^\delta}, \end{aligned} \quad (44)$$

where (e) follows from the FKG inequality [35, Theorem 10.13], since both  $\prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} e^{-s P_f |\mathbf{w}_f \mathbf{f}_{\hat{z}o}|^2 / D_{\hat{z}o}^\alpha}$  and  $\prod_{z \in \Phi_f \setminus o} e^{-s P_t |\mathbf{w}_f \mathbf{f}_{zo}|^2 / D_{zo}^\alpha}$  are decreasing random variables as the number of terms increases; (f) holds for realizing that both  $\hat{\Phi}_f \setminus \hat{o}$  and  $\Phi_f \setminus o$  are PPPs with the same density  $\lambda_f$  due to the displacement theorem [35, page 35] and invoking [11, (8)].

Substituting (40) and (44) into (9) and invoking [32, Theorem 1], we obtain the lower bound  $\mathcal{P}_t^L$ .

An upper bound for  $\mathcal{P}_t$  can be obtained by calculating an upper bound for  $\mathcal{L}_{I_f}$ . From (42), we have

$$\begin{aligned} \mathcal{L}_{I_f}(s) &\stackrel{(g)}{\leq} \mathbb{E}_{\hat{\Phi}_f} \left[ \prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} \frac{1}{(1 + P_f s D_{\hat{z}o}^{-\alpha})^2} \right] \mathbb{E}_{\Phi_f \setminus o} \left[ \prod_{z \in \Phi_f \setminus o} \frac{1}{(1 + P_t s D_{zo}^{-\alpha})^2} \right] \\ &\stackrel{(h)}{=} \exp \left( -\lambda_f C_{\alpha,2} \frac{1+\delta}{2} (P_f s)^\delta (1 + P_{tf}^\delta) \right), \end{aligned} \quad (45)$$

where (g) follows from the Cauchy-Schwarz inequality and (h) holds for the PGFL over a PPP. Substituting (40) and (45) into (9) and invoking [32, Theorem 1], we obtain the upper bound  $\mathcal{P}_t^U$ .

### C. Proof of Theorem 3

Let  $r \triangleq D_{\hat{o}e}$ . Substituting (15) into (5) and applying the PGFL over a PPP yield

$$\mathcal{P}_{so} = 1 - \exp \left( -\lambda_e \int_0^\infty \int_0^{2\pi} \mathbb{P} \{ \text{SIR}_e \geq \beta_e \} r d\theta dr \right). \quad (46)$$

Define  $v \triangleq r^\alpha \beta_e / P_f$ ,  $\mathbb{P} \{ \text{SIR}_e \geq \beta_e \}$  in (46) can be calculated by invoking [33, (11)], i.e.,

$$\mathbb{P} \{ \text{SIR}_e \geq \beta_e \} = \mathbb{E}_{\Phi_f} \left[ \frac{1}{W} \sum_{n=0}^{N_e-1} w_n v^n \right], \quad (47)$$

where  $W = (1 + P_t D_{oe}^{-\alpha} v) \prod_{z \in \Phi_f \setminus o} (1 + P_t D_{ze}^{-\alpha} v)$ , and  $w_n$  is the coefficient of  $v^n$  in  $W$ , which is

$$w_n = \sum_{i=0}^{\min(n,1)} \frac{(P_t D_{oe}^{-\alpha})^i}{(n-i)!} \sum_{z_1, \dots, z_{n-i} \in \Phi_f \setminus o} \prod_{j=1}^{n-i} \frac{P_t}{D_{z_j e}^\alpha}. \quad (48)$$

Substituting  $W$  and  $w_n$  into (47), we have

$$\begin{aligned} \mathbb{P} \{ \text{SIR}_e \geq \beta_e \} &= \mathbb{E}_{\Phi_f} \left[ \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,1)} \frac{1}{(n-i)!} \times \frac{(P_t D_{oe}^{-\alpha})^i}{(1 + P_t D_{oe}^{-\alpha} v)} \sum_{z_1, \dots, z_{n-i} \in \Phi_f \setminus o} \frac{P_t^{n-i} v^{n-i} \prod_{j=1}^{n-i} D_{z_j e}^{-\alpha}}{\prod_{z \in \Phi_f \setminus o} (1 + P_t D_{ze}^{-\alpha} v)} \right] \\ &= \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,1)} \frac{(P_t D_{oe}^{-\alpha})^i}{(1 + P_t D_{oe}^{-\alpha} v) (n-i)!} \times \mathbb{E}_{\Phi_f} \left[ \sum_{z_1, \dots, z_{n-i} \in \Phi_f \setminus o} \frac{P_t^{n-i} v^{n-i} \prod_{j=1}^{n-i} D_{z_j e}^{-\alpha}}{\prod_{z \in \Phi_f \setminus o} (1 + P_t D_{ze}^{-\alpha} v)} \right], \end{aligned} \quad (49)$$

where the expectation term can be calculated by using Campbell-Mecke theorem [36, Theorem 4.2]

$$\begin{aligned} &\mathbb{E}_{\Phi_f} \left[ \sum_{z_1, \dots, z_{n-i} \in \Phi_f \setminus o} \frac{P_t^{n-i} v^{n-i} \prod_{j=1}^{n-i} D_{z_j e}^{-\alpha}}{\prod_{z \in \Phi_f \setminus o} (1 + P_t D_{ze}^{-\alpha} v)} \right] \\ &= \left( 2\pi \lambda_f \int_0^\infty \frac{P_t v r^{-\alpha}}{1 + P_t v r^{-\alpha}} r dr \right)^{n-i} \times \exp \left( -2\pi \lambda_f \int_0^\infty \frac{P_t v r^{-\alpha}}{1 + P_t v r^{-\alpha}} r dr \right) \\ &\stackrel{(i)}{=} (C_{\alpha,2} \lambda_f P_t^\delta v^\delta)^{n-i} \exp(-C_{\alpha,2} \lambda_f P_t^\delta v^\delta), \end{aligned} \quad (50)$$

where (i) is obtained by transforming  $P_t v r^{-\alpha} \rightarrow \mu$  and invoking formula [37, (3.241.2)]. Substituting (49) and (50) into (46) and using  $D_{\hat{o}e} = \sqrt{D_{oe}^2 + D_f^2 - 2D_{oe}D_f \cos \theta_o}$ , we complete the proof.

### D. Proof of Corollary 3

As  $D_f \rightarrow 0$ ,  $\mathcal{Q}_i(r) = 2\pi (P_{tf}\beta_e)^i / (1 + P_{tf}\beta_e)$ . Let  $A \triangleq C_{\alpha,2}\lambda_f (P_{tf}\beta_e)^\delta$ . Substituting  $\mathcal{Q}_i(r)$  into (16) yields

$$\begin{aligned} \mathcal{P}_{so} &= 1 - \exp \left( -\lambda_e \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,1)} \frac{A^{n-i}}{(n-i)!} \times \right. \\ &\quad \left. \frac{2\pi (P_{tf}\beta_e)^i}{1 + P_{tf}\beta_e} \int_0^\infty r^{2(n-i)} e^{-Ar^2} r dr \right) \\ &\stackrel{(j)}{=} 1 - \exp \left( -\lambda_e \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,1)} \frac{\pi (P_{tf}\beta_e)^i}{A(1 + P_{tf}\beta_e)} \right) \\ &= 1 - \exp \left( -\frac{\pi \lambda_e}{A(1 + P_{tf}\beta_e)} \sum_{n=0}^{N_e-1} (1 + P_{tf}\beta_e)^n \right), \quad (51) \end{aligned}$$

where (j) holds for  $\int_0^\infty r^{2(n-i)} e^{-Ar} r dr = \frac{(n-i)!}{A^{n-i+1}}$ . Substituting  $A$  into (51) completes the proof.

### E. Proof of Theorem 4

To complete the proof, we need only derive the optimal  $\lambda_f$ , denoted by  $\lambda_f^*$ , that maximizes  $F(\lambda_f)$  in the range  $[\lambda_f^L, \infty)$ . Clearly, if  $0 < \lambda_f^L \leq \lambda_f^U$ , the solution to problem (24) is  $\lambda_f^* = \min(\lambda_f^*, \lambda_f^U)$ ; otherwise, there is no feasible solution. For convenience, we omit subscript  $f$  from  $\lambda_f$ . Define  $f_1(\lambda) = 1 + X(1 + Y\lambda)^{-\frac{\alpha}{2}} > 1$ ,  $f_2(\lambda) = 1 + Z\lambda^{-\frac{\alpha}{2}} > 1$  and  $f(\lambda) = \ln \frac{f_1(\lambda)}{f_2(\lambda)}$ , then the objective function in (24) changes into  $F(\lambda) = \lambda f(\lambda)$ . The first-order derivative of  $F(\lambda)$  on  $\lambda$  is given by

$$F^{(1)}(\lambda) = f(\lambda) + \lambda f^{(1)}(\lambda) = f(\lambda)G(\lambda). \quad (52)$$

The introduced auxiliary function  $G(\lambda)$  in (52) is defined as  $G(\lambda) = 1 + \frac{\lambda f^{(1)}(\lambda)}{f(\lambda)}$ , where

$$f^{(1)}(\lambda) = \frac{f_1^{(1)}(\lambda)}{f_1(\lambda)} - \frac{f_2^{(1)}(\lambda)}{f_2(\lambda)}, \quad (53)$$

with  $f_1^{(1)}(\lambda) = -\frac{\alpha(f_1(\lambda)-1)Y}{2(1+\lambda Y)}$  and  $f_2^{(1)}(\lambda) = -\frac{\alpha(f_2(\lambda)-1)}{2\lambda}$ . Note that  $f(\lambda)$  in (52) is positive, such that the sign of  $F^{(1)}(\lambda)$  remains consistent with that of  $G(\lambda)$ . First, we investigate the sign of  $F^{(1)}(\lambda)$  at the boundaries of  $[\lambda_f^L, \infty)$ . A complete expression of  $F^{(1)}(\lambda)$  is given by substituting (53) into (52)

$$F^{(1)}(\lambda) = \ln \frac{f_1(\lambda)}{f_2(\lambda)} + \frac{f_1(\lambda)[f_2(\lambda) - 1] - \lambda[f_1(\lambda) - f_2(\lambda)]Y}{\delta f_1(\lambda)f_2(\lambda)(1 + \lambda Y)}. \quad (54)$$

Case  $\lambda = \lambda_f^L$ : We have  $f_1(\lambda^L) = f_2(\lambda^L)$ , such that  $F^{(1)}(\lambda^L) = \frac{f_1(\lambda^L)[f_1(\lambda^L)-1]}{\delta f_1^2(\lambda^L)(1+\lambda^L Y)} > 0$ .

Case  $\lambda \rightarrow \infty$ : We have  $\lim_{\lambda \rightarrow \infty} f_1(\lambda) = 1$  and  $\lim_{\lambda \rightarrow \infty} f_2(\lambda) = 1$ , such that  $\lim_{\lambda \rightarrow \infty} F^{(1)}(\lambda) = \frac{[f_2(\lambda)-1]-\lambda[f_1(\lambda)-f_2(\lambda)]Y}{\delta(1+\lambda Y)}$ . Substituting  $f_1(\lambda)$  and  $f_2(\lambda)$  into  $\lim_{\lambda \rightarrow \infty} F^{(1)}(\lambda)$  yields

$$\begin{aligned} \lim_{\lambda \rightarrow \infty} F^{(1)}(\lambda) &= \lim_{\lambda \rightarrow \infty} Z\lambda^{-\alpha/2} \left( 1 - \frac{X}{Z} Y \left( \frac{\lambda}{1 + \lambda Y} \right)^{\alpha/2+1} \right) \\ &= \lim_{\lambda \rightarrow \infty} Z\lambda^{-\alpha/2} \left( 1 - \frac{X}{Z} Y^{-\alpha/2} \right) < 0, \quad (55) \end{aligned}$$

where the last inequality holds for  $\lambda_f^L = 1 / \left( (X/Z)^\delta - Y \right) > 0 \Rightarrow (XY^{-\alpha/2})/Z > 1$ . The above two cases also indicate that  $G(\lambda^L) > 0$  and  $\lim_{\lambda \rightarrow \infty} G(\lambda) < 0$ .

Directly proving the monotonicity of  $F^{(1)}(\lambda)$  (or the concavity of  $F(\lambda)$ ) w.r.t.  $\lambda$  from (52) is quite difficult. We observe that, supposing  $G(\lambda)$  monotonically decreases with  $\lambda$ , there obviously exists a unique  $\lambda^*$  that makes  $F^{(1)}(\lambda)$  first positive and then negative after  $\lambda$  exceeds  $\lambda^*$ . That is, we may prove that  $F(\lambda)$  is a first-increasing-then-decreasing function of  $\lambda$ . Invoking the definition of the single-variable quasi-concave function [38, Sec. 3.4.2],  $F(\lambda)$  is actually a quasi-concave function of  $\lambda$ ; the given  $\lambda^*$  is the optimal solution that maximizes  $F(\lambda)$ , which is obtained at  $F^{(1)}(\lambda) = 0$ . Based on the above discussion, in what follows we focus on proving the monotonicity of  $G(\lambda)$  w.r.t.  $\lambda$ . We first compute the first-order derivative of  $G(\lambda)$  on  $\lambda$

$$G^{(1)}(\lambda) = \frac{f^{(1)}(\lambda)f(\lambda) + \lambda f^{(2)}(\lambda)f(\lambda) - \lambda (f^{(1)}(\lambda))^2}{f^2(\lambda)}. \quad (56)$$

Computing  $G^{(1)}(\lambda)$  requires computing  $f^{(2)}(\lambda)$ , which can be obtained from (53)

$$\begin{aligned} f^{(2)}(\lambda) &= \frac{f_1^{(2)}(\lambda)f_1(\lambda) - (f_1^{(1)}(\lambda))^2}{f_1^2(\lambda)} \\ &\quad - \frac{f_2^{(2)}(\lambda)f_2(\lambda) - (f_2^{(1)}(\lambda))^2}{f_2^2(\lambda)}, \quad (57) \end{aligned}$$

where  $f_1^{(2)}(\lambda) = \frac{(\alpha/2+1)(f_1(\lambda)-1)Y^2}{\delta(1+\lambda Y)^2}$  and  $f_2^{(2)}(\lambda) = \frac{(\alpha/2+1)(f_2(\lambda)-1)}{\delta\lambda^2}$  are the second-order derivatives of  $f_1(\lambda)$  and  $f_2(\lambda)$ , respectively, substituting which into (57) further yields

$$\begin{aligned} f^{(2)}(\lambda) &= \frac{(f_1(\lambda) - 1)(f_1(\lambda) + \alpha/2)Y^2}{\delta(f_1(\lambda))^2(1 + \lambda Y)^2} \\ &\quad - \frac{(f_2(\lambda) - 1)(f_2(\lambda) + \alpha/2)}{\delta\lambda^2(f_2(\lambda))^2}. \quad (58) \end{aligned}$$

Substituting (53) and (58) into (56) yields

$$\begin{aligned} G^{(1)}(\lambda) &= \frac{1}{f(\lambda)} \left\{ -\frac{(f_1(\lambda) - 1)Y}{\delta f_1(\lambda)(1 + \lambda Y)} + \frac{(f_2(\lambda) - 1)}{\delta\lambda f_2(\lambda)} + \right. \\ &\quad \frac{\lambda(f_1(\lambda) - 1)(f_1(\lambda) + \alpha/2)Y^2}{\delta f_1^2(\lambda)(1 + \lambda Y)^2} - \frac{(f_2(\lambda) - 1)(f_2(\lambda) + \alpha/2)}{\delta\lambda f_2^2(\lambda)} \\ &\quad \left. - \frac{\lambda}{f(\lambda)} \left( -\frac{(f_1(\lambda) - 1)Y}{\delta f_1(\lambda)(1 + \lambda Y)} + \frac{(f_2(\lambda) - 1)}{\delta\lambda f_2(\lambda)} \right)^2 \right\}. \quad (59) \end{aligned}$$

Using the inequality  $f(\lambda) = \ln \frac{f_1(\lambda)}{f_2(\lambda)} \leq \frac{f_1(\lambda)}{f_2(\lambda)} - 1$  and after some algebraic manipulations, we obtain

$$\begin{aligned} G^{(1)}(\lambda) &\leq -\frac{f_1^2(\lambda)}{\delta f(\lambda)} [f_2(\lambda) - 1] - \frac{\lambda f_1(\lambda)Y}{\delta f(\lambda)} \times \\ &\quad \left( (f_2(\lambda)[f_1(\lambda) - 1] + \alpha[f_2(\lambda) - 1][f_1(\lambda) - f_2(\lambda)]) \right. \\ &\quad \left. - \frac{\lambda^2 f_2(\lambda)Y^2}{\delta f(\lambda)} [f_2(\lambda) - 1][f_1(\lambda) - f_2(\lambda)]^2 \right). \quad (60) \end{aligned}$$

Given that  $f_1(\lambda) > f_2(\lambda) > 1$ , all the coefficients of  $Y^i$  for  $i = 0, 1, 2$  in the right-hand side (RHS) of (60) are negative, such that  $G^{(1)}(\lambda) < 0$ . This means  $G(\lambda)$  is a monotonically



decreasing function of  $\lambda$  in the range  $[\lambda_f^L, \infty)$ . By now, we have completed the proof.

### F. Proof of Theorem 5

The proof is similar to Appendix B; the only difference lies in computing  $\mathcal{L}_{I_f}(s)$ , which is obtained from (27) and (44)

$$\begin{aligned} \mathcal{L}_{I_f}(s) &= \mathbb{E}_{\Phi_f} \left[ \prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} e^{-s \left( \frac{P_f |\tilde{\mathbf{w}}_f \tilde{\mathbf{f}}_{\hat{z}o}|^2}{D_{\hat{z}o}^\alpha} + \frac{P_t \|\tilde{\mathbf{w}}_f \mathbf{F}_{zo} \tilde{\mathbf{F}}_z\|^2}{N_j D_{\hat{z}o}^\alpha} \right)} \right] \geq \\ &\mathbb{E}_{\Phi_f} \left[ \prod_{z \in \Phi_f \setminus o} e^{-\frac{s P_f |\tilde{\mathbf{w}}_f \tilde{\mathbf{f}}_{zo}|^2}{D_{zo}^\alpha}} \right] \mathbb{E}_{\hat{\Phi}_f} \left[ \prod_{\hat{z} \in \hat{\Phi}_f \setminus \hat{o}} e^{-\frac{s P_t \|\tilde{\mathbf{w}}_f \mathbf{F}_{zo} \tilde{\mathbf{F}}_z\|^2}{N_j D_{\hat{z}o}^\alpha}} \right] \\ &\stackrel{(k)}{=} e^{-C_{\alpha,2} \lambda_f D_f^2} e^{-C_{\alpha,N_j+1} (P_{tf}/N_j)^\delta \lambda_f D_f^2}, \end{aligned} \quad (61)$$

where (k) holds for [11, (8)] combined with  $\|\tilde{\mathbf{w}}_f \mathbf{F}_{zo} \tilde{\mathbf{F}}_z\|^2 \sim \Gamma(N_j, 1)$ . Substituting (40) and (61) into (9) and invoking [32, Theorem 1], we complete the proof.

### G. Proof of Theorem 6

Following (46), we first compute  $\mathbb{P}\{\widetilde{\text{SIR}}_e \geq \beta_e\}$ . Recalling (32), each term in  $\tilde{\mathbf{R}}_e$ , e.g.,  $\mathbf{G}_{ze} \tilde{\mathbf{F}}_z \tilde{\mathbf{F}}_z^H \mathbf{G}_{ze}^H$ , can be regarded as a superposition of single-stream signals with  $N_j$  co-located interferers. Denote the  $n$ -th column of  $\mathbf{G}_{ze} \tilde{\mathbf{F}}_z$  by  $\tilde{\mathbf{g}}_{ze,n}$ , then  $\mathbf{R}_{e,N_t,N_j}$  can be reformated as

$$\tilde{\mathbf{R}}_e = \frac{P_t}{N_j} \sum_{n=1}^{N_j} \frac{\tilde{\mathbf{g}}_{oe,n} \tilde{\mathbf{g}}_{oe,n}^H}{D_{oe}^\alpha} + \sum_{z \in \Phi_f \setminus o} \frac{P_t}{N_j} \sum_{n=1}^{N_j} \frac{\tilde{\mathbf{g}}_{ze,n} \tilde{\mathbf{g}}_{ze,n}^H}{D_{ze}^\alpha}. \quad (62)$$

Define  $r \triangleq D_{oe}$  and  $z \triangleq r^\alpha \beta_e P_f$ .  $\mathbb{P}\{\text{SIR}_{e,N_t,N_j} \geq \beta_e\}$  is obtained by invoking [33, (11)], i.e.,

$$\mathbb{P}\{\widetilde{\text{SIR}}_e \geq \beta_e\} = \mathbb{E}_{\Phi_f} \left[ \frac{1}{W_{N_j}} \sum_{n=0}^{N_e-1} y_n z^n \right], \quad (63)$$

where  $W_{N_j} = \left(1 + \frac{P_t}{N_j} r^{-\alpha} z\right)^{N_j} \prod_{z \in \Phi_f \setminus o} \left(1 + \frac{P_t}{N_j} D_{ze}^{-\alpha} z\right)^{N_j}$  and  $y_n$  is the coefficient of  $z^n$  in the polynomial expansion of  $W_{N_j}$ . Define  $\tilde{A} \triangleq C_{\alpha,N_j+1} \lambda_f (P_{tf} \beta_e / N_j)^\delta$ . Invoking [34, Theorem 1] yields

$$\begin{aligned} \mathbb{P}\{\widetilde{\text{SIR}}_e \geq \beta_e\} &= \sum_{n=0}^{N_e-1} \sum_{i=0}^{\min(n,N_j)} \binom{N_j}{i} \left(\frac{P_{tf} \beta_e}{N_j}\right)^i \times \\ &\sum_{j=1}^{|\xi_{n-i}|} \frac{\Xi_{j,n-i}(-\tilde{A} r^2)^{|\xi_{j,n-i}|} e^{-\tilde{A} r^2}}{(1 + P_{tf} \beta_e / (N_j))^{N_j}}, \end{aligned} \quad (64)$$

Substituting (64) into (46) and using  $D_f \rightarrow 0$  and formula [37, (3.326.2)], we complete the proof.

### REFERENCES

- [1] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40-47, Feb. 2012.
- [2] N. Yang, L. Wang, G. Geraci, M. El-kashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.
- [3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.
- [4] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215-4227, Sep. 2010.
- [5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.
- [6] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.
- [7] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741-1755, May 2015.
- [8] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3545, Jul. 2012.
- [9] H.-M. Wang, M. Luo, and Q. Yin, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics & Security*, vol. 8, no. 12, pp. 2007-2020, Dec. 2013.
- [10] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical tier security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, Mar. 2014.
- [11] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Select. Areas Commun.*, vol. 27, no. 7, pp. 1029-1046, Sep. 2009.
- [12] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299-1302, Aug. 2014.
- [13] M. Ghogho and A. Swami, "Physical-tier secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," in *Proc. IEEE ICC Workshops*, Jun. 2011, pp. 1-5.
- [14] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM Int. Symp. Mobile Ad Hoc Network. Comput.*, Chicago, IL, USA, 2010, pp. 21-30.
- [15] X. Zhou, R. Ganti, J. Andrews, and A. Hjørungnes, "On the throughput cost of physical tier security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764-2775, Aug. 2011.
- [16] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 11, pp. 1802-1814, Nov. 2013.
- [17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.
- [18] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.
- [19] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. on Commun.*, vol. 63, no. 11, pp. 4347-4362, Nov. 2015.
- [20] T.-X. Zheng, and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. on Veh. Technol.*, to appear.
- [21] C. Wang, H.-M. Wang, X.-G. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596-2612, May 2015.
- [22] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: to relay or to jam," *IEEE Trans. Inf. Forensics & Security*, vol. 10, no. 2, pp. 293-307, Feb. 2015.
- [23] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296-4307, Nov. 2012.
- [24] D. W. K. Ng, E. S. Lo, and R. Schober, "Dynamic resource allocation in MIMO-OFDMA systems with full-duplex and hybrid relaying," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1291-1304, May 2012.
- [25] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983-5993, Dec. 2011.
- [26] A. Sabharwal et al., "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637-1652, Sep. 2014.
- [27] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628-1631, Oct. 2012.

- [28] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical tier secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962-4974, Oct. 2013.
- [29] W. Li, Y. Tang, M. Ghogho, J. Wei, C. Xiong, "Secure communications via sending artificial noise by both transmitter and receiver: Optimum power allocation to minimize the insecure region," *IET Commun.*, vol. 8, no. 16, pp. 2858-2862, Mar., 2014.
- [30] I. Krikidis, H. A. Suraweera, P. J. Smith, and C. Yuen, "Full-duplex relay selection for amplify-and-forward cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4381-4393, Dec. 2012.
- [31] Z. Tong, and M. Haenggi, "Throughput analysis for full-duplex wireless networks with imperfect self-interference cancellation," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4490-4500, Nov. 2015.
- [32] A. M. Hunter, J. G. Andrews, S. Weber, "Transmission capacity of ad hoc networks with spatial diversity," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5058-5071, Dec. 2008.
- [33] H. Gao, P. J. Smith, and M. V. Vlark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666-672, May, 1998.
- [34] R. H. Y. Louie, M. R. McKay, N. Jindal, and I. B. Collings, "Spatial multiplexing with MMSE receivers in ad hoc networks," in *Proc. IEEE ICC*, Kyoto, Japan, June, 2011, pp. 1-5.
- [35] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge University Press, 2012.
- [36] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. John Wiley and Sons, 1996.
- [37] I. S. Gradshteyn, I. M. Ryzhik, A. Jeffrey, D. Zwillinger, and S. Technica, *Table of Integrals, Series, and Products*, 7th ed. New York: Academic Press, 2007.
- [38] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U. K.: Cambridge Univ. Press, 2004.